COMMERCIAL SALES OF MILITARY TECHNOLOGIES

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JUNE 4, 2009

Serial No. 111–43

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
73–750 WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California, *Chairman*

JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
CHRISTOPHER S. MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
BETTY SUTTON, Ohio
BRUCE BRALEY, Iowa
PETER WELCH, Vermont

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
PARKER GRIFFITH, Alabama
ROBERT E. LATTA, Ohio

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

BART STUPAK, Michigan, *Chairman*

BRUCE L. BRALEY, Iowa
Vice Chairman
EDWARD J. MARKEY, Massachusetts
DIANA DEGETTE, Colorado
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
DONNA M. CHRISTENSEN, Virgin Islands
PETER WELCH, Vermont
GENE GREEN, Texas
BETTY SUTTON, Ohio
JOHN D. DINGELL, Michigan *(ex officio)*

GREG WALDEN, Oregon
Ranking Member
ED WHITFIELD, Kentucky
MIKE FERGUSON, New Jersey
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas

CONTENTS

COMMERCIAL SALES OF MILITARY TECHNOLOGIES

THURSDAY, JUNE 4, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2322 of the Rayburn House Office Building, Hon. Bart Stupak (chairman) presiding.

Members present: Representatives Stupak, Braley, Markey, DeGette, Doyle, Welch, Green, Sutton, Walden, Burgess, Blackburn, and Gingrey.

Staff present: David Rapallo, General Counsel; Theodore Chuang, Chief Oversight Counsel; Dave Leviss, Deputy Chief Investigative Counsel; Scott Schloegel, Investigator, Oversight & Investigations; Stacia Cardille, Counsel; Jennifer Owens, Special Assistant; Earley Green, Chief Clerk; Caren Auchman, Communicates Associate; Kenneth Marty, Detailee HHS–IG; Alan Slobodin, Minority Chief Counsel; Karen Christian, Minority Counsel; Peter Keethy, Minority Legal Analyst; and Scott Sherrill, Minority Detailee.

OPENING STATEMENT OF HON. BART STUPAK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. STUPAK. This meeting will come to order. Today we have a hearing titled, "Commercial Sales of Military Technologies." The Chairman, Ranking Member, and Chairman emeritus will be recognized for 5 minutes opening statement. Other members of the subcommittee will be recognized for 3 minute opening statements. I will begin.

Less than 2 weeks ago North Korea detonated a nuclear weapon during an underground test. North Korea is now threatening to test fire an intercontinental ballistic missile capable of striking Alaska.

At the same time our Nation remains at war in Iraq and Afghanistan, and here at home we are faced with the threat of attack from Al Qaeda and other terrorist groups. In 2009, the world is a very dangerous place.

Today we will examine two specific ways we may be allowing our national security to be compromised; domestic sales and illegal export of military and scientific technology overseas.

In 2008, our committee began investigating controls on the export of military and dual-use technology, technology that has both

military and commercial uses. As part of our investigation we asked the Government Accountability Office to conduct undercover testing to determine how vulnerable we are to covert acquisition and export of our sensitive technology. The results are troubling.

We will hear today how GAO established a fictitious company led by a fictitious individual who acquired 12 different military or dual-use items that are subject to export control laws. The GAO was able to obtain several devices used in the nuclear weapons program, including a triggered spark gap, which is a high-voltage switch that can be used as a nuclear weapon detonator, an accelerator meter, an instrument used to measure motions generated by nuclear and chemical explosives, and a GyroChip, a device that can be used to stabilize and steer guided missiles.

The GAO also successfully acquired several pieces of military equipment that give our troops technological superiority in battle, including night-vision scope used by our troops to see and track enemy in the dark, body armor, the type used by U.S. military in battle, and an F-16 engine-monitoring system computer.

The GAO will explain how 12 out of the 12 of the companies approached 100 percent agreed to sell these sensitive items to the fictitious company. None of these companies discovered that the company was fake. None of the companies determined that the buyer was a fake person. In fact, none of the companies ever met the buyer, and most conducted the transactions entirely by e-mail.

The company that manufactures the night-vision scope even signed up GAO's fake company as an authorized distributor of its product. The only thing more surprising than the ease at which GAO acquired the sensitive equipment is the fact that it was apparently entirely legal. When questioned afterwards, the companies involved explained that they were not required by current law to apply for an export license when selling specific military or dual-use products directly to domestic purchasers. There is no requirement for them to conduct any background check or due diligence on the buyers, much less submit the proposed sale to the government for a license to purchase.

The Commerce Department, which testify today, agrees that no violations occurred. This is obviously not a satisfactory result. GAO illustrated the weaknesses of this legal regime when it turned around and successfully exported some of these items simply by sending them to the Fed Ex and sending them overseas. GAO sent them to a country known as a trans-shipment point for military and nuclear technology. So there is an enormous loophole in our law.

We will hear today from GAO, the Department of Commerce, and three of the companies that sold these products to GAO, either as a manufacturer or a seller. We will ask them the following questions: Are some military items so sensitive that they should be banned from commercial sales to the public entirely? Are some military or dual-use items sensitive enough to require licenses for domestic sales? Can additional controls be put in place to make it more difficult for our enemies to gain access to our sensitive military and dual-use technologies?

The stakes cannot be higher. A 2008, report by the Strategic Studies Institute reveals that in the past North Korea has sought

to procure from foreign sources at least one of the products GAO acquired, the accelerator meter to enhance its guided missile program.

I look forward to the testimony today and hope we can discuss ways in which the government and business can work together to ensure our technological advantage is not used to jeopardize the safety of our troops, our allies, and our communities here at home.

I next turn to Mr. Walden for his opening statement.

I should just mention, members are going to be coming in and out. We have another hearing down on the first floor. In fact, I may have Diana DeGette or someone take the chair for me as I am going to have to go down to that hearing also. But Mr. Walden, your opening statement, please, sir.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Thank you very much, Chairman Stupak, for convening this hearing.

Since this country was attacked almost 8 years ago on September 11, we have become all too aware of the fact that terrorist groups that are constantly seeking to exploit any weakness in our national security and to gain any access to America's advanced technology. Any information they might gain about United States intelligence or military operations could potentially be used to attack our men and women in uniform abroad and here at home. This threatens our national security.

In Iraq we have heard on the news too many times the cases where terrorists posed as Iraqi soldiers or police in order to get close to military checkpoints or barracks, only to detonate improvised explosive devices and suicide bombs, sometimes killing U.S. soldiers as well as civilians in the process. We cannot ignore the link between illegal exports and military items and such attacks.

For example, in 2008, various individuals and companies were indicted for purchasing items capable of being used to make IEDs with Iran being the final destination. For fiscal year 2008, the Department of Justice reported that 145 defendants were charged for criminal violations of export control laws. About 43 percent of the defendants charges were attempting to illegally transport or transfer items to Iran and China.

Since 2007, GAO has included ensuring effective protection of technologies critical to the U.S. national security interests as high-risk areas. As troubling as those weaknesses may be, what is more disturbing is there appears to be a gigantic loophole in our laws that make it easier for our enemies to get ahold of our sensitive military technology and one day use it against us.

The loophole the GAO uncovered in this investigation reveals that the military and sensitive dual-use technology can be easily and legally bought within the United States. Then those items can be illegally exported with almost zero chance of detection. Here is how easy it is to make these buys.

GAO bought a number of sensitive dual-use items from United States companies, including night-vision goggles, body armor, and F–16 engine computer and technology used in nuclear weapons and IEDs. Dual use means these items have both military and commer-

cial use. You can see some of these items displayed right up here on this table in the front of the room.

The GAO did so by setting up a bogus company, a company Web site, a mail drop box. They also used fake military ID to facilitate the purchase, and the fake military ID from what I am told was even not very well constructed.

When GAO purchased these items, in many cases they weren't asked a single question by the seller about what they were doing with the items. There was no face-to-face contact and sometimes not even contact over the phone. The companies in most cases did not make an attempt to verify the minimal information that GAO provided.

But here is the rub. The companies did absolutely nothing illegal. They did not violate the law because no law or regulation places any meaningful restriction on the domestic sale of these military items. That is right. You, Joe Q. Public, can buy a body armor, night-vision goggles, and F–16 engine computer, and our laws do not require any kind of verification for your identity or background.

However, if you then tried to export the items, you would need to go get a license to do so. Now, how many of you really thing that an Al Qaeda operative or some other terrorist is going to be the first in line at the Department of Commerce or State to get a license to ship these items to say, oh, China, Syria, or Iran. I don't think so either.

This may be one of those rare oversight hearings where we show not how the law has been broken or evaded by a bad actor but how the law is simply inadequate. In other words, the scandal here may be what is legal, not what is illegal.

Now that we have identified this gap in our laws, it is our responsibility to figure out how to close it. Now, to do it in a way that does not place an undue burden on Commerce. As I mentioned before, these are dual-use, sensitive items. These items have legitimate, critical uses sometimes in medical and aircraft equipment. My understanding is the companies here today and the other companies who sold dual-use items to the GAO are very concerned these items might fall into enemy hands and want to help solve this problem.

I look forward to hearing their thoughts about what we can do about it.

Mr. Chairman, our men and women in uniform deserve the best technology that our country's industry has to offer. They deserve to know that when they are on the battlefield, they have every advantage over the enemy, and that includes the best technology our industry can produce.

So I look forward to working with you to figure out how we can make sure that these dual-use items don't fall into the wrong hands and put our men and women and civilians in peril.

I yield back the balance of my time.

Mr. STUPAK. Thank you, Mr. Walden.

Mr. Markey for an opening statement, please.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. Thank you, Mr. Chairman, and thank you so much for having this important hearing.

Every day the United States superiority in high technology is on display in our military, our universities, our computer and software manufacturers, and our healthcare industry, and every day the United States is under assault by foreign countries and groups that seek to acquire U.S. technologies and products that threaten U.S. national security.

Our Export Control System is woefully inadequate to ensure that high technology U.S. goods are not misused either for conventional military or WMD purposes. As we will hear today undercover GAO investigators used fake information to purchase dangerous dual-use technologies, including some which could be useful for a nuclear weapons program. Clearly, our export control program must be strengthened.

The particular loophole which GAO exploited in their investigation is frighteningly simple. While exports of dual-use technologies require a government license, domestic sales of the exact same sensitive items are not regulated in any way whatever. GAO was able to provide false information, mask its identity, and pretend to be a qualified domestic purchaser. Clearly foreign countries or terrorist groups could do the same thing. And as GAO proved, a cardboard box and the U.S. Postal Service is all it takes to move dual-use items out of the country.

We must strengthen our Export Control System, but private industry must also play a cooperative and constructive role. Private companies can and must assist the government by identifying questionable orders and reporting them to law enforcement for action.

In this context I would like to say a word about Perkin Elmer, one of the companies which will testify today and is headquartered in my district. GAO was able to purchase a sensitive item, potentially abused to a nuclear weapons program from Perkin Elmer, but given the domestic sales loophole the GAO exploited, Perkin Elmer seems to have followed the law.

An event in 2003 demonstrates how Perkin Elmer has helped prevent dangerous export control violations. When the company received an order for 200 triggered spark gaps, alarm bells sounded at the large quantity requested. Perkin Elmer reported the order to law enforcement, and at the request of federal authorities the company played along with the order, eventually shipping sabotaged products which were then traced. At the end of the day a plot to acquire a key technology for the Pakistani nuclear weapons program was thwarted in large part because of Perkin Elmer.

That is the kind of cooperation that we need to be successful. To keep the American people safe, we now have to make sure that we close this domestic loophole so that we ensure that we have a uniform policy to protect against this kind of proliferation of dangerous technology.

Thank you, Mr. Chairman, for having this hearing.

Mr. STUPAK. Thank you, Mr. Markey.

Next we will hear from Ms. DeGette for an opening statement. Three minutes, please.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you very much, Mr. Chairman.

To say what we are going to hear today from the GAO is troubling is an understatement. We live in a world where pirates are seizing U.S. flagged cargo ships off the Somali coast, a world where North Korea is desperate to get its hands on any components or weapons that allow its regime to maintain its position as a long-term, legitimate threat to international security. Additionally, the United States and its allies have serious concerns about Iran's nuclear program.

Yet here we are after decades of problems being identified related to America's export control process, once again learning about the gaps in our system. It is difficult enough to make sure our military men and women are equipped and able to defend themselves against the IEDs made by our adversaries with the materials they have obtained. The President's budget demonstrates the magnitude of the issues being raised by this hearing and includes increased funding, and I quote, "to expand operations targeting the illicit procurement in the U.S. of U.S. origin items for the use in improvised explosive devices, IEDs being employed against U.S. troops."

OK. So a system that allows material which can be used to build an IED or detonate a nuclear device to be available on the open market and over the internet is just simply not a functioning system at all. Voluntary industry compliance and government-issued guidance for businesses is great when it works. It hasn't worked entirely in the area of food safety, and in this case it doesn't seem to be working at all.

I have no doubt that our witnesses from the Department of Commerce share our concerns and that the Bureau of Industry and Security is making efforts to improve its system, and I want to emphasize that I am sympathetic to workforce challenges that might be discussed during this debate. However, this committee is interested in seeing the Bureau of Industry and Security address all of the concerns identified by the GAO and Congress in a systemic and coordinated fashion and fast.

Unfortunately, I am afraid that anything less than 100 percent compliance in this area represents too serious a threat at a time when we are using vast resources to confront terrorists and other adversaries overseas.

And with that, Mr. Chairman, I yield back.

Mr. STUPAK. Thank you, Ms. DeGette.

Mr. Braley for an opening statement, please, sir. Three minutes.

OPENING STATEMENT OF HON. BRUCE L. BRALEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF IOWA

Mr. BRALEY. Thank you, Mr. Chairman and Ranking Member Walden, for holding this hearing today to examine commercial sales of technology with military applications and U.S. export control programs.

I have serious concerns about the GAO's findings through their undercover investigation that sensitive dual-use and military technology can easily and legally be purchased from dealers and manufacturers in the United States and exported without detection. I believe that these disturbing findings have serious implications for our national security and for American troops working to keep us safe overseas.

I think most Americans would be alarmed to learn that by using a fake company and fictitious identities GAO investigators were able to purchase items that could potentially be used for the development of nuclear and chemical weapons, guided missiles, and improvised explosive devices which have been frequently used to attack our troops in Iraq and Afghanistan.

They were also able to purchase military-grade radios, night-vision goggles, and infrared flags, which could potentially be used against U.S. troops in combat. GAO investigators were also able to export dummy versions of some of these items without detection to a country which is a known transshipment point to terrorist organizations and foreign governments attempting to acquire sensitive military technology.

These findings are even more disturbing when you consider the frequency with which terrorists and criminal organizations and foreign governments attempt to obtain these types of sensitive technologies from manufacturers and distributors in the United States. The Department of Justice recently reported that foreign states and criminal and terrorist organizations seek arms, technology, and other materials to advance their technological capacity on a daily basis.

Given this information and the ease with which the GAO was able to purchase and export sensitive items, you can't help but worry about how many times these attempts have been successful and about what that could mean for our national security. GAO's findings demonstrate a clear lack of regulation over the domestic sales of military and dual-use technologies and serious loopholes in our Export Control System. That is why I look forward to hearing the testimony of our witnesses today and hearing the witnesses' recommendations on how we in Congress can improve safeguards for domestic sales and improve our export control programs to make sure that these potentially dangerous items don't end up in the wrong hands.

As the GAO's investigation clearly demonstrates, improving these safeguards is essential to protecting our troops serving overseas and to protecting every American.

And with that I yield back.

Mr. STUPAK. Thank you, Mr. Braley.

Mr. Gingrey, opening statement, please. Three minutes.

OPENING STATEMENT OF HON. PHIL GINGREY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. GINGREY. Mr. Chairman, thank you.

Today the subcommittee will have an opportunity to shine a spotlight on a very, very critical but less visible aspect of our national defense; preventing the export of sensitive military technology, particularly to individuals in countries that wish us harm.

Mr. Chairman, we expend a lot of time, effort, and resources trying to stop dangerous materials from being brought into this country, however, the failure to properly oversee what is being taken out of this country may pose an equal, if not greater, threat to our national security.

Mr. Chairman, American manufacturing components and products should never be allowed to be used against this Nation or its citizens. Yet it seems that this could be a very real possibility and a threat that must be addressed. As we move forward I hope that we can reach a consensus on the best course of action needed to ensure this threat never becomes a reality.

While national defense should remain our first and foremost concern, we must also approach this question with a keen eye and some commonsense. While we need to ensure sufficient safeguards, we should also provide for a streamline and a safe process to expedite legitimate sales for commercial and strategic purposes, particularly when trading with our allies.

American businesses and manufacturers are hurting, and the simple and stark reality is that over 95 percent of the world's consumers live as we know outside of the United States. Accordingly, Mr. Chairman, we must commit ourselves to adopting a sound security policy that also strengthens the ability of American manufacturers to be successful in the global marketplace.

Mr. Chairman, I look forward to carefully listening to the testimony from the witnesses today, and with that I will yield back my time.

Mr. STUPAK. Thank you, Mr. Gingrey.

Ms. Sutton from Ohio, opening statement, please.

OPENING STATEMENT OF HON. BETTY SUTTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Ms. SUTTON. Thank you, Mr. Chairman, and thank you for holding this important hearing on the commercial sale of military technology.

Comprehensive oversight and complete control of the sale of sensitive defense and dual-use military technologies is absolutely essential to our national security. It is imperative that the responsible federal agencies exert every available resource to prevent our sensitive technologies from ending up in the hands of terrorists. And it is more than disturbing to learn what investigators have brought to light. The dangerous implications are extraordinarily serious.

The Department of State and Department of Commerce have primary jurisdiction over export controls. It is apparent that the two agencies do not, however, have clear lines drawn when it comes down to jurisdiction on an individual product.

For instance, a development company in Ohio tested an undersea robot in U.S. and international waters with no immediate intention of foreign sales. To cover all bases, they reached out to the agencies to see whose jurisdiction their product would fall into in the event that they decided to apply for an export license. Depending on who answered the phone, the company received a different answer. In the end they were disappointed that they were not able to secure

a concrete answer regarding which agency had jurisdiction over their product.

Now, I am left to believe that this problem exists with countless products, and I support Ms. Lasowski's call for a fundamental reexamination of the current programs and processes within the agencies that have jurisdiction over export controls. And once that examination is completed, I look forward to working with my colleagues to ensure agency procedures are fluent, effective, and that the safety of our Nation is guaranteed.

Today I look forward to hearing from our panel, and I am especially interested in hearing from GAO on their investigative report on domestic sales. We will hear that there are no rules or authorities in place to regulate the domestic sale of sensitive military technologies. Companies are able to make domestic sales of sensitive items with little or no restrictions unless self-imposed, and that is disturbing. The idea that a U.S. citizen can legally purchase and then rather easily mail a sensitive item that would otherwise have to be granted a license for export is shocking.

Mr. Chairman, while our men and women in uniform are bravely serving overseas, the Federal Government has no tool in place to regulate domestic purchases of sensitive military technologies that could be used by terrorists and others against our service members.

I look forward to working with my colleagues to ensure that the proper oversight and regulations are in place for all commercial sales of sensitive military technologies.

Thank you, again, Mr. Chairman, and I yield back.

Mr. STUPAK. Thank you.

Ms. Blackburn, opening statement.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Ms. BLACKBURN. Thank you, Mr. Chairman, and I will be brief. I want to welcome our witnesses. Some of you are returning, and we welcome you back. I am certain you all have already heard. We have a TELCOM hearing that is taking place downstairs, so some of us are going to be up and down and back and forth. So we ask that you please be patient with us.

And I do thank you, Mr. Chairman, for the hearing today, and I think it is appropriate that our committee today examine the process that we go through for selling our military's sensitive technologies to U.S. residents. These buyers could potentially export them to a country that is adverse to U.S. national security, and we are aware of that, and of course we are concerned about that.

The apparent gap is the tracking of the item by the seller and the security background of the buyer. Proper collection of information on these sales should be placed as a high priority for this Administration, but it must not violate privacy rights of U.S. citizens.

Even though domestic sales pose a problem, the regulations of foreign sales should also be reexamined, and I think that is an imperative for us. Over the past 2 decades we do know that some military technologies and equipment were exported to China. That could pose national security risks. That is on our radar as we go through this hearing today. A few examples are anti-jamming and

encryption for military satellite systems and advanced U.S. computers.

The U.S. military, we know, is the strongest in the world, and a significant part of that strength is due to innovation into superior military technology. So we must not allow gaps in our system that will allow this technology to fall into the wrong hands.

We appreciate the information that you are bringing to us today. Mr. Chairman, I thank you for the time, and I yield back.

Mr. STUPAK. Thank you.

Mr. Doyle is going to be up here shortly. He is down in the Health Committee, but he wanted to make an opening statement for a particular issue that affects his district directly and what has—with the sales of some items, and when he comes up without objection we will allow him to make that opening statement.

Hearing no objection we will allow him to do so.

We will move forward with our hearing. So of the members present that concludes our opening statements. Our first panel of witnesses, we are going to have one panel today. They are all before us. Let me introduce them before we swear them in.

Mr. Gregory Kutz, who is the Managing Director of the Forensic Audits and Special Investigations at the Government Accountability Office. Ms. Anne-Marie Lasowski, who is the Director of Acquisition and Sourcing Management of the Government Accountability Office. Mr. Matthew Borman, who is the Acting Assistant Secretary for Export Administration in the Bureau of Industry and Security at the U.S. Department of Commerce. Mr. Thomas Madigan, who is the Acting Deputy Assistant Secretary for Export Enforcement in the Bureau of Industry and Security of the U.S. Department of Commerce. Mr. Michael Alvis, who is the Vice President of Business Development at ITT Industries. Mr. John Roush, who is the Senior Vice President and President for Environmental Health at Perkin Elmer. And Mr. Nicholas Fitton, who is the Chief Executive Officer of the Section 8 Corporation.

Gentlemen, Ladies, it is the policy of the subcommittee to take all testimony under oath. Please be advised that you have the right under the rules of the House to be advised by counsel during your testimony.

Before I go much further, Mr. Burgess, did you want to do an opening? We were holding open for Mr. Doyle, and I knew you had mentioned you wanted—did you want to do an opening or——

Mr. BURGESS. If it is not out of order.

Mr. STUPAK. It is not out of order. I will swear the witnesses in in a minute. I just introduced the panel. I will swear them in after your opening, and then maybe Mr. Doyle will be here.

So if you want to go ahead.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. Well, thank you, Mr. Chairman.

The advancements this country has made with regards to military technology surpasses those of any other nation. Investment in military ingenuity has led to cutting edge commercial advancements in avionics and healthcare.

Contrary to popular belief, the United States military actually created the technology that led to the advent of the internet as opposed to that other guy who said he invented it. Most importantly, these technological advancements have contributed to the safety of our citizens, but it has also placed a high burden on our various federal agencies to ensure the safe production and sale of these sensitive technologies.

While there are laws that expressly prohibit the direct sales of our most sensitive military technologies to foreign countries or entities, the laws which govern the domestic sales of these items are far weaker than they could be. In fact, some component parts to manufacture weapons of mass destruction may be sold domestically and then potentially resold internationally with little or no accountability under the law.

Currently most of these companies undergo voluntary due diligence to ensure the sales of items on the Commerce Control List are then not resold to foreigners, but in this global world in which we live today controls must be in place throughout the transaction process to ensure that the counterparty corporations are legitimate. We cannot ignore the fact that there are groups trying to reverse engineer our technology and use them directly against our men and women in uniform.

For instance, the Navy's Grumman F–14 Tomcat immortalized in the movie, "Top Gun," this technology was considered to be of such strategic importance that only one foreign purchaser was ever allowed to procure the F–14; the Imperial Iranian Air Force that existed during the reign of the Shah. We all know that in 1979, the monarchy fell. Since then the United States has essentially severed all relations with Iran, including imposing an embargo on the sale of any spare parts for the F–14s. Yet shadow companies have ordered parts for the Iranian Tomcats, and no one seems to have been paying attention to what parts were being sold and to whom.

We must make certain our standards for export are as rigorous as our standards for import. We must make certain that the Department of Commerce, Bureau of Industry and Security, implements true post-market verifications of sales. We must make certain that the Department of State, working in conjunction with the Department of Homeland Security, ensures that no exports are being made of our sensitive military technology.

We must also work with the Federal Trade Commission to ensure that Commerce is unimpeded, and for those who would violate our existing laws, those who would compromise the security of our Nation, but more importantly compromise the courageous lives of our men and women in uniform, they should be prosecuted by the Department of Justice to the fullest extent under the law.

Thank you, Mr. Chairman. I will yield back my time.

Mr. STUPAK. Thanks, Mr. Burgess.

As I was saying to our panel, under the rules of the House you have the right to be represented by counsel. Do any of you wish to be represented by counsel? Anyone?

OK. You are all shaking your head no, so we will take it as a no.

So, therefore, I am going to ask you to please rise, raise your right hand, and take the oath.

[Witnesses sworn.]

Mr. STUPAK. Let the record reflect the witnesses replied in the affirmative. Each of you are now under oath.

We will now hear a 5-minute opening statement from you, and thank you for being here. We are going to try to do this one panel, and we will start with you, Mr. Kutz. You are a veteran. If you want to hit your mike and start with your opening statement, and we would appreciate it.

TESTIMONY OF GREGORY KUTZ, MANAGING DIRECTOR, FORENSIC AUDITS AND SPECIAL INVESTIGATIONS, GOVERNMENT ACCOUNTABILITY OFFICE; ANNE–MARIE LASOWSKI, DIRECTOR, ACQUISITION AND SOURCING MANAGEMENT, GOVERNMENT ACCOUNTABILITY OFFICE; MATTHEW BORMAN, DEPUTY ASSISTANT SECRETARY, BUREAU OF INDUSTRY AND SECURITY, DEPARTMENT OF COMMERCE; THOMAS MADIGAN, DIRECTOR OF THE OFFICE OF EXPORT ENFORCEMENT, BUREAU OF INDUSTRY AND SECURITY, DEPARTMENT OF COMMERCE; MICHAEL ALVIS, VICE PRESIDENT FOR BUSINESS DEVELOPMENT, ITT INDUSTRIES; JOHN ROUSH, SENIOR VICE PRESIDENT AND PRESIDENT, ENVIRONMENTAL HEALTH, PERKIN ELMER; AND NICHOLAS FITTON, CHIEF EXECUTIVE OFFICER, SECTION 8

TESTIMONY OF GREGORY KUTZ

Mr. KUTZ. Mr. Chairman and members of the subcommittee, thank you for the opportunity to discuss the sale of military and dual-use technology.

There are widespread reports of the illegal transfer of U.S. technology to Iran, China, and terrorist organizations. Today's testimony highlights the results of our investigation into the credibility of this security threat.

My testimony has two parts. First, I will briefly discuss what we did and provide some background, and second, I will discuss the results of our investigation.

First, Justice has reported numerous cases of foreign governments and terrorist organizations seeking to acquire U.S. technology. Items identified in criminal cases are suitable for military, nuclear, guided missile, and improvised explosive device applications. As you have all mentioned, these items can legally be sold within the United States.

The objective of our investigation was to make undercover purchases of technology here in the U.S. If successful, we plan to ship several of these items overseas. To set up this operation we established a bogus front company called Monacasey Tech Consultants. We also used bogus identities and undercover credit card and a mailbox as our business address. Most of the items that we targeted for purchase are identical to items cited in recent criminal cases.

Although we had a limited budget and relatively simply backstops, our operation could have easily been financed by foreign governments or terrorists organizations seeking to acquire U.S. technology.

Moving onto the results of our investigation. We were able to purchase a number of sensitive U.S. military and dual-use items. We then successfully shipped several of these items by mail undetected to southeastern Asia.

The items that we purchased are displayed on the table before you, and I have a few with me I am going to show you by hand. It is important to note that for many of these items our bogus individuals signed a certificate promising not to export them.

Let me discuss several of the more troubling dual-use items that we purchased, and they will also be shown on the monitors.

First, in my hand I have a triggered spark gap. We purchased this item for $700 from the manufacturer. We also received a price quote for an additional 100 of these items. In addition to medical applications, these items can be used to detonate nuclear weapons. In 2005, this item was cited as part of a criminal case involving illegal export to Pakistan.

Second, I have in my hand an accelerometer. We purchased this item for $2,800 from the manufacturer. In addition to having commercial applications, this item can be used in smart bombs and nuclear and chemical explosive applications. In 2007, this item was cited as part of a criminal case involving illegal export to China.

And third, I have in my hand this GyroChip. We purchased this item for $3,100 from the manufacturer. We also obtained a price quote for an additional ten of these items. In addition to commercial use, these items can be used to help steer guided missiles. A large corporation was recently found to have illegally exported 85 of these items to China.

Examples of the sensitive military items purchased include, first, the modular tactical vest body armor you see on my right in front of me and also shown on the monitors. We purchased this item for $2,400 from a distributor. We also received a price quote for an additional 20 of these vests.

Also displayed in front of me are ESAPI plates that we purchased on eBay as part of a prior investigation and could have also purchased from this same distributor. These vests are currently used by the U.S. Marines in Iraq and Afghanistan.

And second, the night-vision monocular I have in my hand. We purchased this item for $3,600 from a distributor. As was mentioned, we also became an authorized distributor of this item. These items are currently used by the military in nighttime operations. Recent criminal cases show that these items are in demand, not only by China and Iran, but by the terrorist organization, Hezbollah, in Lebanon.

In conclusion, our work clearly shows that anybody with a credit card, computer, and a mailbox that is willing to lie can acquire U.S. military and dual-use technology. For the dual-use items they are more difficult to address but additional controls at the point of sale for high-risk items should be considered. For military items we continue to believe that the technology used by our soldiers today should not be available to anybody with a credit card. Our soldiers deserve better than to have our own technology used against them on the battlefield.

Mr. Chairman, this ends my statement. I look forward to your questions.

[The prepared statement of Mr. Kutz follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, June 4, 2009

MILITARY AND DUAL-USE TECHNOLOGY

Covert Testing Shows Continuing Vulnerabilities of Domestic Sales for Illegal Export

Statement of Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations

GAO-09-725T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-09-725T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

Terrorists and foreign governments regularly attempt to obtain sensitive dual-use and military technology from manufacturers and distributors within the United States. Although the Department of State (State) or Department of Commerce (Commerce), or both, must grant approval to export sensitive military and dual-use items, publicly reported criminal cases show that individuals can bypass this requirement and illegally export restricted items such as night-vision goggles. In the wrong hands, this technology poses a risk to U.S. security, including the threat that it will be reverse engineered or used directly against U.S. soldiers.

Given the threat, the subcommittee asked GAO to conduct undercover tests to attempt to (1) purchase sensitive dual-use and military items from manufacturers and distributors in the United States; and (2) export purchased items without detection by domestic law-enforcement officials.

To perform this work, GAO used fictitious individuals, a bogus front company, and domestic mailboxes to pose as a buyer for sensitive items. GAO, in coordination with foreign law-enforcement officials, also covertly attempted to export dummy versions of items. GAO interviewed relevant agencies to gain an understanding of which items were in demand by terrorists and foreign governments. GAO actions were not designed to test controls of other countries. Relevant agencies were also briefed on the results of this work.

View GAO-09-725T or key components. For more information, contact Gregory Kutz at (202) 512-6722 or kutzg@gao.gov.

June 4, 2009

MILITARY AND DUAL-USE TECHNOLOGY

Covert Testing Shows Continuing Vulnerabilities of Domestic Sales for Illegal Export

What GAO Found

GAO found that sensitive dual-use and military technology can be easily and legally purchased from manufacturers and distributors within the United States and illegally exported without detection. Using a bogus front company and fictitious identities, GAO purchased sensitive items including night-vision scopes currently used by U.S. soldiers in Iraq and Afghanistan to identify targets, triggered spark gaps used to detonate nuclear weapons, electronic sensors used in improvised explosive devices, and gyro chips used in guided missiles and military aircraft. Interviews with cognizant officials at State and Commerce and a review of laws governing the sale of the types of items GAO purchased showed there are few restrictions on domestic sales of these items.

GAO was also able to export a number of dummy versions of these items using the mail to a country that is a known transshipment point for terrorist organizations and foreign governments attempting to acquire sensitive technology. Due to the large volume of packages being shipped overseas, and large volume of people traveling overseas, enforcement officials within the United States said it is impossible to search every package and person leaving the United States to ensure sensitive technologies are not being exported illegally. As a result, terrorists and foreign governments that are able to complete domestic purchases of sensitive military and dual-use technologies face few obstacles and risks when exporting these items. The table below provides details on several of the items GAO was able to purchase and, in two cases, illegally export without detection.

Sensitive Items Purchased by GAO Using Fictitious Identities

Item	Use	Notes
Gyro chip	Dual-use – Used in advanced aircraft, missile, space and commercial systems for stabilization, control, guidance, and navigation	• In 2006, company paid a $15 million civil penalty for the export of civil aircraft containing a gyro chip to China • The gyro chip is fully self contained, lightweight, and has a virtually unlimited life • GAO exported without detection
Night-vision monocular	Military – Used by U.S. troops to identify targets in nighttime operations	• In 2006, criminal convictions for two people involved in export of night-vision devices to the terrorist group Hezbollah • GAO's bogus company became a certified distributor for the item, gaining access to an unrestricted quantity. • Contains an image intensifier tube made to military specifications
Accelerometer	Dual use – Accelerometers are suitable for use in "smart" bombs and for measuring motions generated by nuclear and chemical explosives	• Item is in high demand by foreign countries and was the subject of a 2007 U.S. Immigration and Customs Enforcement investigation • In 2007, an individual was sentenced for conspiracy to smuggle military-grade accelerometers from the United States to China • GAO exported without detection

Source: GAO

Mr. Chairman and Members of the Subcommittee:

Terrorists and foreign governments regularly attempt to obtain sensitive dual-use[1] and military technology from manufacturers and distributors within the United States. Recently the Department of Justice (DOJ) reported that, on a daily basis, foreign states as well as criminal and terrorist groups seek arms, technology, and other material to advance their technological capacity. With the United States producing advanced technology, it has become a primary target of these illegal technology-attainment efforts. For fiscal year 2008, DOJ publicly reported more than 145 defendants faced criminal charges for violations of export-control laws. Roughly 43 percent of the defendants charged in these cases were attempting to illegally transfer items to Iran or China. For example, a 2007 undercover investigation by the U.S. Immigration and Customs Enforcement (ICE) agency revealed that an individual in Connecticut attempted to purchase and illegally export an accelerometer to China. According to the indictment, this accelerometer is suitable for use in smart bombs and for measuring motions generated by nuclear and chemical explosives. In another example, in 2008, various individuals and companies were indicted on federal charges for purchasing items capable of being used to construct Improvised Explosive Devices (IED), including inclinometers, and exporting these items to multiple transshipment points, with Iran being the final destination. These types of items have been, and may continue to be, used against U.S. soldiers in Iraq and Afghanistan. In addition, we have identified weaknesses in the effectiveness and efficiency of government programs designed to protect critical technologies while advancing U.S. interests. Since 2007, we have included ensuring the effective protection of technologies critical to U.S. national security interest as a high-risk area.[2]

While the U.S. State Department (State) and Commerce Department (Commerce) each have jurisdiction over the export of certain items to countries outside the United States, many of these same items can be purchased legally within the United States. In a testimony before another congressional committee in 2008, we described how our undercover agents were able to purchase sensitive items such as F-14 Tomcat aircraft parts, night-vision goggles currently being used by U.S. forces, and

[1]Dual-use items refer to items that have commercial uses as well as military or nuclear proliferation uses.

[2]See GAO, *High-Risk: Series an Update*, GAO-09-271 (Washington, D.C.: Jan, 22, 2009).

current-issue military body armor on commercial internet sites such as eBay and Craigslist.[3] Given the ease at which we were able to buy those items, and the continued attempts by foreign governments and terrorist groups to obtain sensitive technologies from within the United States, the committee asked us to conduct proactive testing to attempt to (1) purchase sensitive dual-use and military items from manufacturers and distributors in the United States; and (2) export purchased items without detection by domestic law-enforcement officials.

To perform this investigation, we spoke with relevant agencies to gain an understanding of which dual-use and military items were in demand by terrorists and foreign governments. Furthermore, we identified publicly disclosed enforcement cases regarding the sale and illegal export of sensitive dual-use and military items. We searched for dual-use and military technology being sold on manufacturers' and distributors' Web sites. We then made domestic purchases of dual-use and military items either through e-mail or the seller's Web site. We did not purchase items from individual persons or commercial auction sites such as eBay or craigslist. We used a bogus front company and fictitious identities when purchasing these items, meaning that we conducted our work with fictitious names and contact information that could not be traced back to GAO. We also established a Web site related to our bogus company and rented domestic commercial mailboxes used to receive purchased items. In some cases, no information other than a name and credit card were used when purchasing a sensitive item. When possible, we obtained written price quotes from manufacturers and distributors for purchases of additional quantities of items we successfully purchased. After purchasing these items in an undercover capacity, we contacted the distributors and manufacturers of the items and informed them of our operation. We then interviewed company officials and performed additional follow-up investigative work. In addition, we coordinated with foreign government officials to covertly export a number of dummy versions of the items we purchased. We discussed the results of our work with officials at State and Commerce, as well as law-enforcement officials within the Department of Defense, DOJ, and the Department of Homeland Security (DHS).

[3]See GAO, *Internet Sales: Undercover Purchases on eBay and Craigslist Reveal a Market for Sensitive and Stolen U.S. Military Items*, GAO-08-644T (Washington, D.C.: Apr. 10, 2008).

We conducted our investigation from May 2008 through June 2009 in accordance with quality standards for investigations as set forth by the Council for Inspectors General on Integrity and Efficiency (CIGIE).

Background

Commerce and State are principally responsible for regulating the export of sensitive dual-use and military items, respectively. Under the authority of the Export Administration Act of 1979,[4] Commerce is responsible for regulating the export of dual-use items that are included in the Commerce Control List (CCL).[5] Specifically, Commerce's Bureau of Industry and Security (BIS) is responsible for regulating the export and reexport of most commercial items. The commercial items BIS regulates are referred to as dual-use items that have both commercial and military or proliferation applications. BIS's export enforcement activities target the most significant threats facing the United States such as the proliferation of weapons of mass destruction and missile delivery systems, terrorism and state sponsors of terror, and diversions of dual-use goods to unauthorized military end uses.

Under the authority of the Arms Export Control Act of 1976,[6] State regulates the export of military items, which are included in the U.S. Munitions List.[7] Generally, items regulated by State require an export license, while items regulated by Commerce do not necessarily require an export license. Whether an export license is required depends on multiple factors including the item being exported, country of ultimate destination, individual parties involved in the export, parties' involvement in proliferation activities, and the technical characteristics and planned end use of the item. Any person or company in the United States that engages

[4]Pub. L. 96-72, 93 Stat. 503, codified as amended at 50 U.S.C. app. §§ 2401–2420. The Act has lapsed and been reauthorized by statute and Executive Order several times. Currently, the Act is in force pursuant to Executive Order 13,222, 66 Fed. Reg. 44,025 (Aug. 22, 2001), which extended the application of the Act under the authority of the International Emergency Economic Powers Act (IEEPA), Pub. L. 95-223, Title II 91 Stat. 1626, codified as amended at 50 U.S.C. §§ 1701–1707. IEEPA provisions are renewed yearly through a presidential determination, the most recent occurring on July 25, 2008 (73 Fed. Reg. 43,603).

[5]The CCL is contained in Supplement No. 1 to Part 774 of the Export Administration Regulations (EAR), 15 C.F.R. § 774.1.

[6]Pub. L. 94-329, Title II, § 212(a)(1), 90 Stat. 744, codified as amended at 22 U.S.C. § 2778.

[7]The U.S. Munitions List is contained in Part 121 of the International Traffic In Arms Regulations (ITAR), 22 C.F.R. §§ 121.1 - .16.

in manufacturing, exporting, or importing U.S. Munitions List items must register with State.[8]

Commerce and State require exporters to identify items that are on the CCL and U.S. Munitions list and, if required, obtain license authorization from the appropriate department to export these items unless an exemption applies. Exporters are responsible for complying with export-controls laws and regulations. When shipping a sensitive dual-use or military item that requires a license, exporters are required to electronically notify DHS's Customs and Border Protection (CBP) officials at the port where the item will be exported, including information on the quantity and value of the shipment, the issued export license number, or an indication that the item is exempt from licensing requirements. Export enforcement agencies including CBP, ICE, the Federal Bureau of Investigation (FBI), Commerce's Office of Export Enforcement (OEE), U.S. Attorney's Office and the Defense Criminal Investigative Service, are involved with inspecting items to be shipped, investigating potential violations of export-control laws, and punishing export-control violators.

U.S. regulations are designed to keep specific military and dual-use items from being diverted to improper end users. However, current regulations focus on the export of these items and do not address the domestic sales of these items. The seller of a U.S. Munitions List item or a CCL item may legally sell the item within the United States, and is under no legal duty to perform any type of due diligence on a buyer. However, if the seller of an item knows or has reason to know that the buyer is representing a foreign government or intends to export the item, then the seller may be liable.[9]

[8]Export often involves the actual shipment of goods or technology out of the United States. Under ITAR, transfers of Munitions List "technical data" to foreign persons within the United States is also considered to be an export. 22 C.F.R. § 120.17(a)(4). Under EAR, release of CCL "technology" to foreign nationals within the United States is considered to be an export to the home country of the foreign national and thus may require an export license. 15 C.F.R. § 734.2(b).

[9]An otherwise legal transaction is prohibited if the seller knows an export violation will occur, pursuant to 15 C.F.R. § 736.2(b)(1) for CCL items and 22 C.F.R. § 127.1(2) for U.S. Munitions List items. Criminal liability may attach under 50 U.S.C. app. § 2410, 50 U.S.C. § 1705, 22 U.S.C. § 2778(c), or general statutes such as 18 U.S.C. § 371.

Sensitive Dual-Use and Military Items Can Be Easily Purchased within the United States Using a Bogus Front Company and Fictitious Identities

We found that sensitive dual-use and military technology can be easily purchased from manufacturers and distributors within the United States. Using a bogus front company and fictitious identities, we purchased[10] sensitive dual-use and military items from the sellers of the items. Based on our legal analysis of the applicable laws and regulations over the domestic sale of sensitive dual-use and military technology, we determined that companies are allowed to make domestic sales of sensitive items with little or no restrictions. Some of the manufacturers and distributors of items we purchased stated that they independently instituted procedures to document the sales of sensitive items, such as requiring buyers to fill out end-user agreements.[11] However, the sellers were not legally required to conduct any research to validate the authenticity of the identification used or the final use of the item. In addition, many of the distributors and manufacturers have received warning letters from Commerce for exporting sensitive items without the required export license.

Items obtained by our fictitious individuals included a night-vision monocular, electronic components used in IEDs, and secure military-grade radios used by U.S. Special Operations personnel. Items we obtained were not only sensitive in nature, but were also in demand by foreign governments and terrorist organizations. Specifically, seven of the sensitive dual-use and military items we obtained during our investigation have been the center of criminal indictments and convictions for violations of export control laws. All items, except the F-16 engine computer, were new and unused. The F-16 engine computer was purchased from a distributor who had obtained the item from the Department of Defense. Table 1 below summarizes the sensitive items we

[10]For several items, we obtained written price quotes in lieu of purchasing the items due to their costs. After obtaining the price quotes, we confirmed with the sellers of the items that our attempted purchases would have been successful once we had made payment arrangements for the items.

[11]End-user agreements refer to documents submitted by the buyer in which the buyer self-certifies the proposed use for the item being purchased, whether the buyer plans to export the item, and whether the buyer plans to resell the item.

obtained during our investigation, followed by detailed case-study narratives.[12]

Table 1: Sensitive Dual-Use and Military Items

Case	Items	Dual-use	Military	Nuclear	IED
Dual-use items					
1	Triggered spark gap	✓		✓	
2	Oscilloscope	✓		✓	
3	Accelerometer	✓	✓	✓	
4	Quadruple differential line receiver	✓	✓		✓
5	Inclinometer	✓	✓		✓
6	Gyro chip	✓	✓		
7	Ka-band power amplifier	✓	✓		
Military items					
8	Infra-red flag		✓		
9	Modular tactical vest (MTV) / enhanced small arms protective inserts (ESAPI)		✓		
10	Night-vision monocular / Night-vision goggles (NVG)		✓		
11	Secure personal radio		✓		
12	F-16 engine computer		✓		

Source: GAO.

Sensitive Dual-Use Items

Using a bogus front company, fictitious identities, and a domestic mailbox we rented, we were able to purchase sensitive dual-use items from distributors and manufacturers. Items that we purchased have commercial applications, but can also be used for other purposes such as in the development of nuclear weapons, guided missiles, and IEDs. The items listed below are subject to export restrictions under either the CCL or

[12]For item 2 (Oscilloscope) we obtained a written price quote in lieu of purchasing the item due to its cost. For the NVG in item 10, we found we could have purchased this same item from the same seller of the Night Vision Monocular. However, since we had purchased this item on previous work, we choose not to purchase this same item again. For item 9 (ESAPI) we found we could have purchased this item from the same seller as the MTV however, since we had purchased this item in previous work we choose not to purchase this same item again. After obtaining the price quotes, we confirmed with the sellers of the items that our attempted purchases would have been successful once we had made payment arrangements for the items.

State's U.S. Munitions List. Many of the items we purchased have also been the center of previously identified unlawful exports to foreign nations.

Sensitive Dual-Use Items with Nuclear Applications

- **Case 1: Triggered Spark Gap.** Triggered spark gaps are versatile high-voltage switches used for medical applications that can also be used as nuclear weapons detonators. Triggered spark gaps have been the center of unlawful exports to Pakistan and India. However, they are completely legal to buy and sell within the United States.

Figure 1: Triggered Spark Gap

Source: GAO.

In January 2009, using a bogus company and a domestic mailbox as a business address, we purchased, via e-mail, a triggered spark gap for the amount[13] of $735 from a manufacturer that is registered in the federal Central Contractor Registration (CCR) database, an approved government supplier via the General Services Administration (GSA) schedule, and a previous target for attempted purchases by foreign nationals. After

[13]Total amounts may include taxes, shipping and handling fees, and service fees.

obtaining the triggered spark gap, we notified the manufacturer of our undercover purchase. During our interview with the manufacturer, company personnel stated they believed that they had sufficient protocols in place to document the sale of their items. The manufacturer requires new customers to complete a certification form where the customer provides their name and the end use of the product they are purchasing. However, because sales of this item are legal domestically, we were able to purchase it with a fictitious name and bogus company, and by providing a valid credit card. With no requirement to do so, the manufacturer did not question our fictitious identity or bogus company and did not inquire further about the end use for our product. While purchasing the triggered spark gap, we also obtained a price quote for up to 100 additional triggered spark gaps. In addition, in 2005, an individual was sentenced to 3 years in prison for conspiring to violate and violating U.S. export restrictions after exporting, using an air freight company, items including triggered spark gaps. Another individual was indicted for conspiring to violate and violating U.S. export restrictions. The two individuals arranged to purchase, and export to Pakistan, several U.S.-origin triggered spark gaps. In order to obtain the triggered spark gaps the individuals falsely indicated that the items were intended for medical use.

- **Case 2: Oscilloscope.** Oscilloscopes are used for displaying the timing, voltages, frequency, and other attributes of electrical signals. In addition, certain oscilloscope versions are capable of being utilized in weapon of mass destruction development and are also export-controlled for antiterrorism reasons. However, oscilloscopes are legal to buy and sell within the United States. During our investigation, we determined that CCL versions of oscilloscopes can be purchased on the Internet from a distributor that is registered in CCR through an online purchase with a credit card. Because this item cost over $7,500, we chose not to purchase it. However, we confirmed with the distributor that we would have been able to purchase an oscilloscope domestically without any verification. In addition, a model of oscilloscope similar to the version we could have purchased was also illegally shipped overseas by the same seller in 2005. Specifically, this seller pled guilty to one felony count of violating the International Emergency Economic Powers Act by exporting an oscilloscope to Israel without a license. This distributor was sentenced to pay a criminal fine in the amount of $50,000, placed on 3 years' probation and ordered to serve 250 hours of community service. In recent years, the oscilloscope manufacturer has received several warning letters from Commerce for exporting oscilloscopes to Pakistan and India without the required license.

- **Case 3: Accelerometer.** Accelerometers are sensors and instruments used for measuring, displaying, and analyzing acceleration and vibration. They can be used on a stand-alone basis, or in conjunction with a data-acquisition system. The version of the accelerometer we purchased is suitable for use in "smart" bombs and for measuring motions generated by nuclear and chemical explosives and, although legal for domestic sale, is export-controlled under CCL restrictions. In January 2009, we purchased an accelerometer from a manufacturer for the amount of $2,766. The manufacturer is registered in CCR and is an approved government supplier through the GSA Schedule. We accomplished the purchase using a fictitious name, bogus company, and domestic mailbox as a business address. We also provided an end-user certification stating that we would use the item for research and development purposes and would not export the item. We met with the manufacturer after our purchase to discuss what we had done and to discuss whether the company implemented any voluntary restrictions over the domestic sales of sensitive items. The manufacturer of the item did not implement controls that are not required by law, and believed that documentation of the sale was appropriate. This type of item is in high demand by foreign countries. For example, a 2007 undercover investigation by ICE revealed that an individual attempted to purchase and illegally export the same type of accelerometer we purchased to China. Specifically, ICE used an undercover company to capture the individual. The individual was sentenced 12 months in prison for his role in conspiring to export the accelerometer.

Dual-Use Items with IED applications

- **Case 4: Quadruple Differential Line Receiver.** The quadruple differential line receiver is used for balanced or unbalanced digital data transmission. The product supports defense, aerospace, and medical applications. In addition, certain versions of quadruple differential receivers have military applications. This item may be legally bought and sold within the United States. In April 2009, we purchased 10 military-grade quadruple differential line receivers from a distributor for the amount of $248. The transaction was accomplished through the company's Internet Web site using a bogus company, fictitious identity, and domestic mailbox as a business address. Because the law did not mandate it, no verification of our identity or description of the use of the product was required. After the purchase we notified the distributor of our undercover purchase. As a result of our undercover purchase, the distributor stated it will consider implementing voluntary controls for the online transactions, but did not provide details on what additional controls it would implement. In addition to our purchase, other individuals have attempted to export a similar item to Iran. Specifically, in 2008, various individuals and companies were indicted on federal charges for purchasing items for IEDs including items similar to a quadruple differential line receiver. The individuals allegedly arranged to export items to multiple transshipment

points, with Iran being the final destination. In addition, we spoke with a Department of Defense official who confirmed similar U.S.-made technology is being found in IEDs. The official stated that terrorist groups are using more advanced IEDs with easy access to this type of technology.

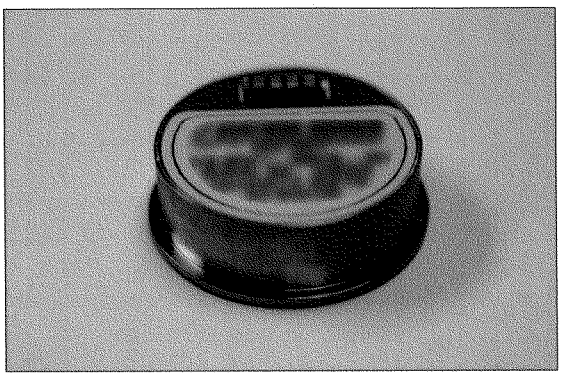
- **Case 5: Inclinometer.** An inclinometer is an instrument used for measuring angles of slope and inclination of an object with respect to its center of gravity. Inclinometers, which are export-controlled but legal to buy and sell within the United States, are suitable for use in the military, medical, optical, range-finder, and robotics fields, and have applications in IEDs. In February 2009, we purchased an inclinometer from a manufacturer for the amount of $548. The manufacturer is registered in CCR and has recently been the target for purchases by individuals shipping inclinometers to Iran. Because it was a domestic purchase, the manufacturer was not required to request an end-user agreement, or question our identity, company, or that our business address was a mailbox. While purchasing the inclinometer, we also obtained a price quote for up to 40 additional inclinometers. In addition, after the purchase we notified the manufacturer of our undercover purchase. When interviewed, the manufacturer correctly stated that he did not identify any Commerce-identified red flags from the undercover transaction.[14] In addition, in 2008, various individuals and companies were indicted on federal charges for purchasing items for IEDs and exporting inclinometers to Iran. Specifically, in 2007, the individuals allegedly purchased inclinometers from the same manufacturer we purchased inclinometers from, and shipped them to multiple transshipment points, with Iran being the final destination.

Other Dual-Use Items

- **Case 6: Gyro Chip.** Gyro chips are sensitive dual-use items used in advanced aircraft, missile, space, and commercial systems for stabilization, control, guidance, and navigation. The gyro chip's original intent was for commercial use; however, this same item is also used to stabilize and steer guided missiles. For this reason, the item is export-controlled, but may be legally bought and sold within the United States without restriction. The device is fully self-contained, extremely small, lightweight, and has virtually unlimited life.

[14]Commerce's BIS publishes a list of "Red Flag Indicators" that may indicate a transaction could lead to a violation of the Export Administration Regulations. A seller who finds a red flag is encouraged to report it to Commerce. Examples of red flags include situations where the item purchased does not fit with the buyer's line of business, the buyer is willing to pay cash for an expensive item where financing is the norm, or the buyer has little or no business background. The full list is available at http://www.bis.doc.gov/enforcement/redflags.htm.

Figure 2: Gyro Chip



Source: GAO.

In February 2009, we purchased a gyro chip from a manufacturer that is registered in CCR for the amount of $3,146. During the purchase process the manufacturer made it clear that the item is subject to ITAR, and if exported would be subject to export restrictions. During the undercover purchase we provided our bogus company's Web site address, listed a domestic mailbox as a business address, and completed a falsified end-user agreement. While purchasing the gyro chip, we also obtained a price quote for an additional 10 gyro chips. In addition, after the purchase we notified the manufacturer of our undercover purchase. We then interviewed the manufacturer, which stated that it conducts extensive training of its personnel on export regulations of items it sells, attends export-regulation conferences, hires export consultants, and conducts internal training to sales representatives on specific procedures to follow while quoting or selling products. However, no validation procedures are required when a domestic sale is made, and therefore the manufacturer did not identify our fictitious identity and company. In addition, in a previous case, State charged a different company with shipping 85 commercial jets overseas many of which went to countries including

China with a gyro chip embedded in the flight control systems. In April 2006, the company agreed to pay $15 million to settle the allegations.[15]

- **Case 7: Ka-Band Power Amplifier.** Ka-band power amplifiers are suited for military radar systems, ground terminals for Ka-band satellite communications systems, and point-to-point communication systems. Ka-band power amplifiers are export-controlled for national security reasons, but legal to buy and sell within the United States. In March 2009, we purchased two Ka-band power amplifiers from a distributor for the amount of $227. The distributor is registered in CCR and was a previous target for purchases by individuals shipping amplifiers to China. Our purchase was made via e-mail and the Internet using a fictitious identity, bogus company, and domestic mailbox as a business address, and by providing an end-user agreement. We completed the agreement using bogus information and stating we would not export the item without obtaining an export license. Because there are no restrictions on the domestic sale of this item, no additional documentation procedures or validation was performed by the distributor prior to our purchase. While purchasing the Ka-band power amplifiers, we also obtained a price quote for up to 99 additional amplifiers. In addition, after the purchase we notified the distributor of our undercover purchase. When we interviewed distributor personnel, they stated their documentation procedures require the customer to complete an end-user agreement; however, they correctly stated they are not required to do this for domestic sales. In 2009, an individual was indicted for exporting several controlled items including this Ka-band power amplifier to China without an export license. Specifically, on three occasions the individual allegedly had someone in the United States ship several controlled items to China, and in one occasion the individual hand-carried the items when flying from the United States to China. In recent years, Commerce issued warning letters to the manufacturer for exporting electronics to China, failure to comply with a license condition, and exporting amplifiers to Germany for sale to China without the required export license.

Sensitive Military Items

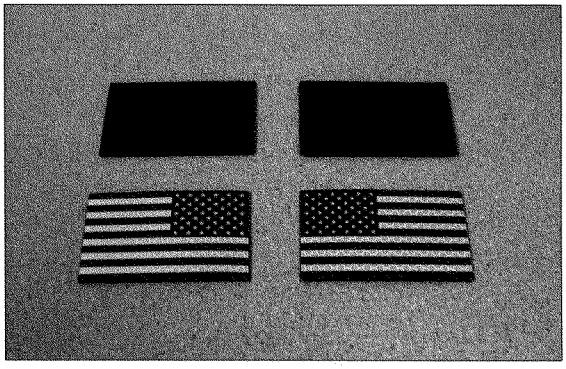
Using a bogus front company, fictitious identities, and a domestic mailbox as our business address, we were able to purchase or otherwise obtain sensitive military items from distributors and manufacturers without

[15]Specific gyro chips are subject to the export licensing jurisdiction of State's Directorate of Defense Trade Controls, unless these specific gyro chips are integrated into and included as an integral part of a commercial primary or standby instrument system. If included as an integral part of a commercial primary or standby instrument system, these specific gyro chips are subject to the CCL.

detection. Some of the items we obtained are subject to State's U.S. Munitions List and have been at the center of unlawful export plots by foreigners. After purchasing and receiving the sensitive military items, we interviewed the sellers regarding the controls they have in place for the sales of their respective items.

- **Case 8: Infra-Red (IR) Flag.** IR flags[16] are currently in use by U.S. military forces to help identify friendly soldiers during nighttime operations. Several of the IR flags we purchased appear as a black material with no identifying markers. However, with the use of U.S. military night-vision technology (such as the monocular we purchased in case 10 below), the patches reveal a U.S. flag, and are the same IR flags used on U.S. military combat uniforms. An enemy fighter wearing these IR flags could potentially pass as a friendly service member during a night combat situation, putting U.S. troops at risk. Nevertheless, these items are completely legal to buy and sell within the United States.

Figure 3: IR Flags



Source: GAO.

[16]The IR flags are also known as IFF (identification of friend or foe) IR U.S. flags.

In September 2008, we purchased various U.S. IR flags from a distributor for the amount of $78. The company's Internet storefront states it specializes in designing modified battle dress uniforms and other military uniform accessories used by modern-day warriors. Specifically, the company's Web site states that Special Forces in Iraq and Afghanistan currently use many of their products. Although there is no legal requirement to do so, the distributor's Internet site stated that the company checks for military identification; however, the seller failed to request identification from our undercover investigator. In the end, our fictitious buyer was only required to provide a name, credit card, and domestic address for shipment to purchase these items. After purchasing and receiving the IR flags, we also obtained a price quote for an additional 400 IR flags. In addition, after the purchase we notified the distributor of our undercover purchase. When interviewed, the distributor of the IR flags stated that it always requests for a copy of a military ID as part of his own voluntary policy and has minimal voluntary controls in place over the sale of the IR tabs. However, the distributor did not request a copy of a military ID as part of our purchase. In addition, we interviewed the distributor's supplier (manufacturer); the manufacturer stated that the distributor is required by their distributorship agreement to ask for a military ID. As a result of this lapse, the manufacturer stated that the distributor will no longer be authorized to sell the IR flags.

- **Case 9: Modular Tactical Vest (MTV) and Enhanced Small Arms Protective Inserts (ESAPI).** The MTV we purchased is a type currently being used by U.S. military personnel and have been tested to National Institute of Justice[17] Level IIIA[18] 9mm velocity. Enemies of the United States could use the vest during attacks against American and coalition forces, and they could also be used by criminals within the United States and on the United States–Mexico border. However, the item is completely legal to sell, buy, or possess within the United States, except by certain violent felons. ESAPIs are ceramic plates that are thicker than the normal SAPIs and increase the protection. These types of ESAPIs are suited for use in the MTV we purchased. The combination of these items could give terrorists or criminals an advantage and protection in combat situations. In September 2008, we purchased an MTV of the type currently in use by

[17]The U.S. Justice Department has created standards of body armor known as the N.I.J. (National Institute of Justice) Standard 0101.06.

[18] Level IIIA is usually the highest threat level in soft body armor. It is usually worn as overt-style armor because of the weight and thickness of the ballistic panels.

the U.S. Marine Corps in Iraq and Afghanistan from a distributor for the amount of $2,417. The distributor is an approved government supplier through the GSA schedule. We purchased the MTV from the distributor's Internet Web site. Although legally not required to do so, the distributor's Web site states that it requires a military ID and completes a verification process before the sale of the equipment. However, we were able to bypass their voluntary requirements using a fictitious military ID. After purchasing and receiving the MTV, we also obtained a price quote for an additional 20 MTVs. In addition, we found that we could have purchased new ESAPI plates, from the same distributor through the same process, which fit into the MTV we purchased. The addition of the e-SAPI plates would have increased the effectiveness of our vest. We chose not to purchase the ESAPI plates because we had purchased similar plates in our prior work.[19] After the purchase, we notified the distributor of our undercover purchase. The distributor stated that it has several voluntary controls in place. Specifically, for our transaction it noticed that the shipping address and billing address were different; therefore, it called the credit card company to verify that the credit card was valid, thinking that would be sufficient to verify that the undercover customer was not bogus. In the past, this distributor has received a warning letter from Commerce for exporting police equipment without the required export license. In addition, the MTV manufacturer was fined $65,000 for the export of military items to Kuwait, Chile, Oman, Trinidad and Tobago, and Saudi Arabia without the required export license.

- **Case 10: Night-Vision Monocular and Night-Vision Goggles (NVG).** The night-vision monocular is a lightweight, self-contained, image-intensification system capable of being either hand-held, mounted to a small arms weapon mounting rail, or mounted to a head mount or helmet mount. Night-vision monoculars are used in nighttime operations by U.S. forces to provide a tactical advantage on the battlefield. They are legal to buy and sell within the United States.

[19]GAO-08-644T.

Figure 4: Night-Vision Monocular

Source: GAO.

In November 2008, we purchased a night-vision monocular of a type that is currently in use by the U.S. military from a distributor that is registered in CCR, for $3,600. The purchase was made using a fictitious identity, bogus company, and domestic mailbox as a business address. During our undercover purchase, the seller certified our bogus company to be a distributor of the item by signing a dealer/reseller agreement. This allowed us to circumvent the seller's voluntary restrictions on only selling the items to military and law-enforcement agencies. As a result, we could have obtained a substantial number of night vision monoculars as part of this agreement. In addition, we also found that we could have purchased new military-specification NVGs, from the same distributor through the same process. We chose not to purchase the NVG because we had purchased a similar NVG in our prior work.[20] After the purchase we notified the distributor of our undercover purchase. When we interviewed distributor personnel, they stated that they have controls in place that are required for the sale of night-vision technology as a part of the distributor agreement. The distributor correctly stated that it is the reseller/dealer's

[20]GAO-08-644T.

responsibility, if exporting an item, to request and obtain export licenses for the subject items and to ensure that the requirements of all applicable export laws and regulations are met. Night-vision technology has been in demand by entities in countries like China, Singapore, Indonesia, Iran, and Hong Kong. For example, on November 14, 2006, BIS issued a Section 11(h) Denial Order against two individuals in connection with their criminal convictions for conspiring to export Commerce- and State-controlled night-vision devices to the terrorist group Hezbollah in Lebanon.

- **Case 11: Secure Personal Radio (SPR).** According to the SPR distributor, the SPR model we obtained, which is being used by U.S. Special Forces personnel, is the latest model with enhanced digitally encrypted capability that has a low probability of detection without the aid of high-tech military radio-interception equipment. The SPR provides secure communications between battlefield personnel with an encryption feature that makes communicating with the radio virtually undetectable. Nevertheless, the item is legal to buy and sell within the United States. In November 2008, we obtained two SPRs with headsets and accessories along with one microphone headset on a loan from a distributor. Specifically, the company loaned, at no cost, our bogus company the two radios for demonstration purposes with the possibility for the undercover company to become a distributor of the SPR radios. The company also offered our undercover investigator a job selling the equipment on a commission basis. Because there are no domestic restrictions on these radios, the company only asked for a copy of a driver's license prior to loaning the radios. After the transaction, we made the distributor aware of the fictitious identity. The distributor acknowledged that it should have shown more voluntary due diligence prior to loaning the radios to our undercover investigator. The distributor stated that it requires an end-user agreement and a copy of identification for documentation purposes, but it performs no other voluntary verification checks. The distributor stated it often receives inquiries from foreign individuals and estimated as much as 30 percent of individuals that register on its Web site are foreign. The distributor told us that it informs these individuals it only sells domestically to military and law-enforcement entities.

- **Case 12: F-16 Engine-Monitoring System Computer (EMSC).** F-16 EMSC processes digital engine-performance signals from the digital electronic-control module. This EMSC is used in more than 75 percent of the USAF's single-engine F-16 Block 50/52 aircraft. Furthermore, the engine that uses this monitoring system is also qualified for use on the F-15 Strike Eagle aircraft and was recently chosen by South Korea to power its new F-15K fighters. This item is export-controlled under ITAR, but is

legal to buy and sell within the United States. In April 2009, using a fictitious identity and bogus company, we purchased, through e-mail, a used F-16 EMSC from an online distributor for the total amount of $570. The distributor had obtained this item from DOD. During the purchase process, we provided a bogus company name, a domestic mailbox as a business address, a copy of our fictitious person's driver license, and a falsified end-user agreement. After obtaining the F-16 EMSC, we notified the seller of our undercover purchase. During our interview with the seller, the official correctly stated that the seller is not required to have any controls in place for the domestic sale of this item; however, for its own voluntary due diligence the seller ran a public-records check on our fictitious person, but did not identify the purchase as suspicious. In recent years, several individuals and companies have been sentenced to probation and received fines in connection with illegal exports of aircraft components to Iran and Libya. In addition to the United States and its allies' fleets of F-16 aircraft, Venezuela's military also has a fleet of F-16s and has recently issued public statements suggesting the country may want to sell its fleet of F-16s to Iran.

Sensitive Dual-Use and Military Items Can Be Easily Exported

We were able to export, without detection by U.S. enforcement officials, a number of dummy versions of sensitive dual-use and military items to a country that is a known transshipment point for terrorist organizations and foreign governments attempting to acquire sensitive technology. Due to the large volume of packages being shipped overseas, large volume of people traveling overseas, and various agencies[21] involved in enforcing export controls, U.S. enforcement officials stated it is impossible to search every package and person leaving the United States to ensure sensitive dual-use and military items are not being exported illegally. The combined effect of the lack of restrictions over domestic sales and the ease of illegal export of these items is that sensitive dual-use and military items can be easily purchased and exported by terrorists or foreign governments without detection.

In order to export our items, we first obtained nonfunctional "dummy" versions of the items through cooperation with the manufacturers. Next, in cooperation with foreign law-enforcement officials, we shipped the items, using commercial mail, in nondescript boxes that did not disclose the true contents of the items contained within the package. The boxes passed

[21]See GAO, *Export Controls: Challenges Exist in Enforcement of an Inherently Complex System*, GAO-07-265 (Washington, D.C.: Dec. 20, 2006).

through U.S. customs controls without being inspected. The location we shipped the items to was a known transshipment point for items being sent to terrorist organizations and other foreign governments. After receiving the unopened packages, the foreign law-enforcement officials shipped the items back to the United States.

When we discussed our covert shipments with State, Commerce, and various law-enforcement agencies responsible for monitoring packages, vehicles, and persons exiting the United States, they were not surprised by our success. Officials from several agencies stated that there is no practical way to ensure that otherwise unsuspicious people, vehicles, or packages leaving the United States that carry or contain export-controlled items can be identified and searched consistently. Officials from Commerce stated that they were aware of similar schemes used by real individuals attempting to illegally export controlled items. In addition, officials from State stated they have programs in place, working in coordination with other government agencies such as ICE, designed to educate manufacturers and distributors about laws and common risks associated with sales of sensitive technology. However, State agreed that it is difficult to prevent items from leaving the country after they are legally sold to an individual within the United States.

Conclusions

A comprehensive network of controls and enforcement is necessary to ensure sensitive technology does not make it into the hands of unauthorized individuals. However, the lack of legal restrictions over domestic sales of these items, combined with the difficulties associated with inspecting packages and individuals leaving the United States, results in a weak control environment that does not effectively prevent terrorists and agents of foreign governments from obtaining these sensitive items. The key to preventing the illegal export of these sensitive items used in nuclear, IED, and military applications is to stop the attempts to obtain the items at the source, because once sensitive items make it into the hands of terrorists or foreign government agents, the shipment and transport out of the United States is unlikely to be detected.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the subcommittee may have at this time.

Appendix I: Scope and Methodology

To perform the undercover test of purchasing sensitive dual-use and military items from manufacturers and distributors in the United States we spoke with relevant agencies and used publicly disclosed enforcement cases regarding the sales and illegal exports of sensitive dual-use and military items. GAO used the information obtained from these sources to determine which sensitive items were in demand by terrorists and foreign governments. We also reviewed the export regulations to determine that manufacturers and distributors are not required to have controls for the domestic sales of sensitive items. We searched for dual-use and military technology being sold on manufacturers' and distributors' Web sites. We then made domestic purchases of dual-use and military items either through e-mail, personal contact, or the seller's Web site. We used a bogus front company, fictitious identities, and domestic mailboxes as our business address when purchasing these items, meaning that we conducted our work with fictitious names and contact information that could not be traced back to GAO. We also established a Web site related to our bogus company and rented domestic commercial mailboxes used to receive purchased items. The bogus company used was incorporated to add more credibility. In some cases, during the purchase process, no information other than a name and credit card were used to purchase a sensitive item. In other cases, we submitted falsified end-user agreements stating the end use of the product and agreeing not to export the sensitive item. On one occasion, we provided a local military unit as the end use of the item and a fictitious military ID we created using commercial computer software. After we purchased the sensitive items, when possible, we obtained written price quotes from manufacturers and distributors for purchases of additional quantities of items we successfully purchased. After successfully purchasing these items in an undercover capacity, we contacted the distributors and manufacturers of the items and informed them of our operation. We did not attempt to purchase items from individual persons or commercial auction sites such as eBay or craigslist. Of the sensitive items disclosed we did not purchase the oscilloscope, enhanced small arms protective inserts, and the night-vision goggles. For these items we obtained written price quotes in lieu of purchasing the items due to their costs or due to the fact we had purchased the item in previous work. After obtaining the prices quotes, we confirmed with the seller of the items that our purchases would have been successful once we had made payment arrangement for the items.

To attempt to export purchased items without detection by domestic law-enforcement officials, we coordinated with foreign government officials to covertly export items out of the United States. We shipped the items to a destination known to be a transshipment point for terrorist organizations

and other foreign governments. We were able to export a number of items. The export process consisted of mailing the dummy versions of items from the United States through commercial package shipment. We falsified the shipment documents provided with the package. When the foreign government officials received the shipment they received specific instructions on how to inspect the shipment to verify that the package was sealed and was not opened or inspected by any U.S. officials. The foreign government officials also received special instructions on how to mail the package to GAO. GAO successfully received all items back from foreign law enforcement officials. We briefed officials at the Departments of State and Commerce, as well as law-enforcement officials within the Departments of Defense, Homeland Security, and Justice on the results of our work and incorporated their comments concerning controls over exported items.

Mr. STUPAK. Thank you, Mr. Kutz, and your investigation is found in a GAO report which is now released publicly based on your testimony? OK. Very good. So it is available.

Ms. Lasowski, did you have an opening statement, please?

TESTIMONY OF ANNE-MARIE LASOWSKI

Ms. LASOWSKI. Yes. Mr. Chairman and——

Mr. STUPAK. Could you just hold that up a little bit and make sure that green light is on. Thank you.

Ms. LASOWSKI. Mr. Chairman and members of the subcommittee, I am pleased to be here today to speak about our work on the U.S. Export Control System, one part of a complex web of programs intended to protect technologies critical to U.S. national security, both military and economic.

In the decade since these programs were established, the world has changed significantly. As you are aware, new security threats, increased globalization, and evolving technology creates significant challenges in maintaining a balance between our military and economic interests. Yet our work has shown that for the most part these programs have been neglected or may not be well equipped to deal with these challenges, prompting GAO to add this area onto our high-risk report in 2007, and calling for a strategic reexamination of existing programs.

My statement today focuses on three key areas that should be part of this reexamination. First, interagency coordination and jurisdictional control, second, export licensing efficiency, and third, system assessments.

With regard to the first area, we found that poor interagency coordination and jurisdictional debates between State and Commerce have weakened export controls over certain sensitive items. For example, Commerce claimed jurisdiction over specialized explosive detection equipment when jurisdiction for this item belonged to State. Consequently, the items were subject to Commerce's less-restrictive export control requirements.

Until such disputes are resolved, it is ultimately the exporter, not the government, who determines the level of government review and control that will follow. This weakness also creates considerable challenges for other players, namely the enforcement community. Without information as fundamental as what items are controlled by which agency and which need a license, enforcement officials are limited in their ability to carry out inspection, investigation, and prosecution responsibilities.

The second area concerns the need for efficiency in the export licensing process. At State medium processing times doubled in 4 years, and license applications reached an all-time high of over 10,000 open cases. Clearly reviews of export license applications require careful deliberation. However, licensing decisions should not be delayed due to process inefficiencies.

Recently State took steps to restructure its workforce and establish standards to reduce processing times and cases in the pipeline. We are encouraged by this action and hope that it will yield needed improvements.

The overall efficiency of Commerce's licensing process is unknown in part due to its limited assessments. While most Com-

merce-controlled exports can occur without a license, it is no less important for Commerce to seek efficiencies where needed. Most recently Commerce has established new performance measures in its fiscal year 2010, budget, which we have not evaluated.

The third and final area of concern is a more fundamental issue; management's due diligence in performance assessments. State and Commerce have argued that no fundamental changes are needed due to their Export Control Systems. We have been somewhat perplexed by this stance, since neither department has conducted a thorough assessment to support this conclusion, and our work has repeatedly demonstrated that the U.S. Export Control System is in need of repair.

Redefined security threats, evolving technology, and increasing globalization, coupled with the numerous weaknesses we have identified demand that the U.S. government step back, assess, and rethink the current system's ability to protect multiple U.S. interest.

Mr. Chairman, this concludes my prepared statement. I would be pleased to respond to any questions that you or members of the subcommittee may have.

[The prepared statement of Ms. Lasowski follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, June 4, 2009

EXPORT CONTROLS

Fundamental Reexamination of System Is Needed to Help Protect Critical Technologies

Statement of Anne-Marie Lasowski, Director
Acquisition and Sourcing Management

GAO-09-767T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-09-767T, a testimony to the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

June 4, 2009

EXPORT CONTROLS

Fundamental Reexamination of System Is Needed to Help Protect Critical Technologies

Why GAO Did This Study

In 2007, GAO designated ensuring the effective protection of technologies critical to U.S. national security interests as a high-risk area. Each year, the Department of Defense spends billions of dollars to develop and produce technologically advanced weaponry. To enhance its foreign policy, security, and economic interests, the U.S. government must approve selling these weapons and defense-related technologies overseas and has a number of programs to identify and protect the critical technologies involved in these sales. These programs include export control systems for weapons and defense-related technologies, the foreign military sales program, and reviews of foreign investments in U.S. companies. Yet, these weapons and technologies continue to be targets for theft, espionage, reverse engineering, and illegal export.

This testimony (1) provides an overview of the safety net of government programs and processes aimed at ensuring the effective protection of technologies critical to U.S. national security interests and (2) identifies the weaknesses and challenges in the U.S. export control system—one of the government programs to protect critical technologies. This statement is based on GAO's high-risk report and its extensive body of work on the government's programs designed to protect technologies critical to U.S. national security interests.

View GAO-09-767T or key components. For more information, contact Anne-Marie Lasowski at (202) 512-4841 or lasowskia@gao.gov.

What GAO Found

U.S. government programs for protecting critical technologies may be ill-equipped to overcome challenges in the current security environment. The eight programs that are intended to identify and protect weapons and defense-related technology exports and investigate proposed foreign acquisitions of U.S. national security-related companies—as well as the myriad of related laws, regulations, policies, and processes—are inherently complex. Multiple agencies participate in decisions about the control and protection of critical technologies, including the Departments of Defense, State, Commerce, Homeland Security, the Treasury, Energy, and Justice. Each agency represents various interests, which at times can be competing and even divergent. Moreover, in the decades since these programs were put in place, globalization and terrorist threats have heightened the challenge of appropriately weighing security and economic concerns.

As with many of the government's programs to protect critical technologies, the U.S. export control system has faced a number of challenges. Specifically, poor interagency coordination, inefficiencies in processing licensing applications, and a lack of systematic assessments have created significant vulnerabilities in the export control system.

- Poor coordination among the agencies involved in export controls has resulted in jurisdictional disputes and enforcement challenges. Notably, State and Commerce—the two regulatory agencies for weapons and defense-related technologies—have disagreed on which department controls certain items. These disagreements create considerable challenges for enforcement agencies in carrying out their inspection, investigation, and prosecution responsibilities. The Department of Justice recently established a task force with other agencies to address jurisdictional and coordination issues in export control enforcement.
- State's backlog of licensing applications topped 10,000 cases at the end of fiscal year 2006. While application reviews may require time to ensure license decisions are appropriate, they should not be unnecessarily delayed due to inefficiencies. Recently, State took steps to restructure its workforce to reduce processing times and the number of open cases.
- Finally, neither State nor Commerce has systematically assessed the overall effectiveness of their export control programs nor identified corrective actions that may be needed to fulfill their missions—despite significant changes in the national security environment. Commerce officials stated they conducted an ad hoc review of its system and determined that no fundamental changes were needed. However, we were unable to assess the sufficiency of this review because Commerce did not document how it conducted the review or reached its conclusions.

As the effectiveness of the system depends on agencies working collectively, we have called for the executive and legislative branches to conduct a fundamental reexamination of the current programs and processes.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me here today to discuss the U.S. export control system—one key program in GAO's high-risk area on ensuring the effective protection of technologies critical to U.S. national security interests.[1] As you know, the Department of Defense spends billions of dollars each year to develop and produce technologically advanced weaponry to maintain superiority on the battlefield. To enhance its foreign policy, security, and economic interests, the U.S. government approves selling these weapons and defense-related technologies overseas and has a number of programs to identify and protect the critical technologies involved in these sales.[2] These programs include the export control systems for weapons and defense-related technologies, the foreign military sales program, and reviews of foreign investments in U.S. companies. Yet, these weapons and technologies continue to be targets for theft, espionage, reverse engineering, and illegal export. In 2007, GAO designated ensuring the effective protection of technologies critical to U.S. national security interests as a high-risk area.

My statement today (1) provides an overview of the safety net of government programs and processes aimed at ensuring the effective protection of technologies critical to U.S. national security interests and (2) identifies the weaknesses and challenges in the U.S. export control system—one of the government programs to protect critical technologies. This statement is based on GAO's high-risk report and our extensive body of work on the export control system and other government programs designed to protect technologies critical to U.S. national security interests. That extensive body of work was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A list of related products that we have recently issued is included at the end of this statement.

[1]Since 1990, GAO has reported on government operations that we identified as "high risk" to help resolve serious weaknesses in areas that involve substantial resources and provide critical services to the public.

[2]For purposes of this testimony, "weapons" refers to defense articles, defense services, and related technical data. "Defense-related technologies" refers to dual-use items, which have both military and civilian applications.

Programs to Protect Critical Technologies May Be Ill-Equipped to Overcome Challenges in the Current Security Environment

The U.S. government has a myriad of laws, regulations, policies, and processes intended to identify and protect critical technologies. Several programs regulate weapons and defense-related technology exports and investigate proposed foreign acquisitions of U.S. national security—related companies (see table 1). Several of these programs are inherently complex. Multiple departments and agencies representing various interests, which at times can be competing and even divergent, participate in decisions about the control and protection of critical U.S. technologies.

Table 1: U.S. Government Programs for the Identification and Protection of Critical Technologies

Agencies	Program's purpose	Legal authority
Militarily Critical Technologies Program		
Department of Defense	Identify and assess technologies that are critical for retaining U.S. military dominance	Export Administration Act of 1979, as amended
Dual-Use Export Control System		
Department of Commerce (Commerce) (lead), Department of State (State), Central Intelligence Agency, and Departments of Defense, Energy, Homeland Security, and Justice	Regulate export of dual-use items by U.S. companies after weighing economic, national security, and foreign policy interests	Export Administration Act of 1979, as amended
Arms Export Control System		
State (lead), and Departments of Defense, Homeland Security, and Justice	Regulate export of arms by U.S. companies, giving primacy to national security and foreign policy concerns	Arms Export Control Act, as amended
Foreign Military Sales Program		
State and Department of Defense (leads), Department of Homeland Security	Provide foreign governments with U.S. defense articles and services to help promote interoperability while lowering the unit costs of weapon systems	Arms Export Control Act, as amended
National Disclosure Policy Process		
State, Department of Defense, and intelligence community	Determine the releasability of classified military information, including classified weapons and military technologies, to foreign governments	National Security Decision Memorandum 119 of 1971

Agencies	Program's purpose	Legal authority
Committee on Foreign Investment in the United States (CFIUS)		
Department of the Treasury (lead), Commerce, Departments of Defense, Homeland Security, Justice, State, Energy (non-voting), and Director of National Intelligence (non-voting)[a]	Investigate the impact of foreign acquisitions on national security and suspend or prohibit acquisitions that might threaten national security	Foreign Investment and National Security Act of 2007; Defense Production Act of 1950, as amended
National Industrial Security Program		
Department of Defense (lead), applicable to other departments and agencies	Ensure that contractors (including those under foreign influence, control, or ownership) appropriately safeguard classified information in their possession	Executive Order No. 12829 of 1993
Anti-Tamper Policy		
Department of Defense	Establish anti-tamper techniques on weapons systems when warranted as a method to protect critical technologies on these systems	Defense Policy Memorandum, 1999

Source: GAO (analysis); cited legal authorities (data).

[a]The committee can also include members the President determines necessary on a case by case basis.

We have previously reported that each program has its own set of challenges—such as poor coordination, inefficient program operations, and a lack of program assessments—challenges that are not always visible or immediate but increase the risk of military gains by entities with interests contrary to those of the United States and of financial harm to U.S. companies. Others, including the Office of the National Counterintelligence Executive, congressional committees, and inspectors general, have also reported on vulnerabilities in these programs and the resulting harm—both actual and potential—to U.S. security and economic interests.

In the decades since these programs were put in place, significant forces have heightened the U.S. government's challenge of weighing security concerns with the desire to reap economic benefits. Most notably, in the aftermath of the September 2001 terrorist attacks, the threats facing the nation have been redefined. In addition, the economy has become increasingly globalized as countries open their markets and the pace of technological innovation has quickened worldwide. Government programs established decades ago to protect critical technologies may be ill-equipped to weigh competing U.S. interests as these forces continue to evolve in the 21st century. Accordingly, in 2007, we designated the effective identification and protection of critical technologies as a

governmentwide high-risk area, and called for a strategic reexamination of existing programs to identify needed changes and ensure the advancement of U.S. interests.

Vulnerabilities and Inefficiencies Undermine the Export Control System's Ability to Protect U.S. Interests

The challenges that we identified in the government's programs to protect critical technologies are evident in the U.S. export control system. Specifically, over the years, we have identified interagency coordination challenges, inefficiencies in the system, and a lack of assessments.

First, the various agencies involved in export controls have had difficulty coordinating basic aspects of the system, resulting in jurisdictional disputes and enforcement challenges. The U.S. export control system for weapons and defense-related technologies involves multiple federal agencies and is divided between two regulatory bodies—one led by State for weapons and the other led by Commerce for dual-use items, which have both military and commercial applications. In most cases, Commerce's controls over dual-use items are less restrictive than State's controls over weapons and provide less up-front government visibility into what is being exported. Because State and Commerce have different restrictions on the items they control, determining which exported items are controlled by State and which are controlled by Commerce is fundamental to the U.S. export control system's effectiveness. However, State and Commerce have disagreed on which department controls certain items. In some cases, both departments have claimed jurisdiction over the same items, such as certain missile-related technologies. Such jurisdictional disagreements and problems are often rooted in the departments' differing interpretations of the regulations and in minimal or ineffective coordination between the departments. Unresolved disagreements ultimately allow exporters to decide whether to approach Commerce or State for approval—preventing the government from determining which restrictions apply and the type of governmental review that will occur. Not only does this create an unlevel playing field and competitive disadvantage—because some companies will have access to markets that others will not, depending on which system they use—but it also increases the risk that critical items will be exported without the appropriate review and resulting protections. Despite these risks, no one has held the departments accountable for making clear and transparent decisions about export control jurisdiction.

Jurisdictional disagreements create considerable challenges for enforcement agencies in carrying out their respective inspection, investigation, and prosecution responsibilities. For example, obtaining timely and complete information to confirm whether items are controlled

and need a license is a challenge. In one case, federal investigative agents executed search warrants based on Commerce's license determination that missile technology—related equipment was controlled. Subsequently, Commerce determined that no license was required for this equipment, and the case was closed. In addition, agencies have had difficulty coordinating investigations and agreeing on how to proceed on cases. Coordination and cooperation often hinge on the relationships individual investigators across agencies have developed. In a positive development, the Department of Justice recently established a task force with other agencies responsible for enforcing export controls to address overlapping jurisdiction for investigating potential violations and poor interagency coordination.

A second challenge relates to licensing inefficiencies that have further complicated the export control system. Despite State's past efforts to improve the efficiency of its process, we reported in 2007 its median processing times for license applications had doubled between fiscal years 2003 and 2006—from 13 days to 26 days—and its backlog of license applications reached its highest level of over 10,000 cases at the end of fiscal year 2006. While reviews of export license applications require time to deliberate and ensure that license decisions are appropriate, they should not be unnecessarily delayed due to inefficiencies nor should they be eliminated for efficiency's sake—both of which could have unintended consequences for U.S. security, foreign policy, and economic interests. Recently, State took steps to analyze its export license process and restructure its workforce to reduce processing times and decrease the number of open cases. While Commerce closed significantly fewer license cases than State in fiscal year 2006—many items Commerce controls do not require licenses for export to most destinations—it is important to understand the overall efficiency of Commerce's licensing process.[3] Yet Commerce has not assessed its licensing review process as a whole.

Finally, neither State nor Commerce have systematically assessed their priorities and approaches to determine the overall effectiveness of their programs nor identified corrective actions that may be needed to fulfill their missions—despite heightened terrorism and increased globalization, which have significantly changed the national security environment. As a

[3]For Commerce, license cases include both export license applications and commodity classification requests. For State, license cases include applications for permanent exports, temporary exports and imports, agreements, license amendments, and jurisdiction determinations.

result, State does not know how well it is fulfilling its mission. Commerce officials acknowledged that they had not comprehensively assessed the effectiveness of dual-use export controls in protecting U.S. national security and economic interests. Instead, they stated they conducted an ad hoc review of the dual-use system after the events of September 2001 and determined that no fundamental changes were needed. We were unable to assess the sufficiency of this review because Commerce did not document how it conducted the review or reached its conclusions. Recently, Commerce established a new measure to assess exporter compliance, which we have not evaluated. To be able to adapt to twenty-first-century challenges, federal programs need to systematically reassess priorities and approaches and determine what corrective actions may be needed to fulfill their missions. Given their export control responsibilities, State and Commerce should not be exceptions to this basic management tenet.

Conclusions

Over the years, we have made numerous recommendations to the relevant agencies, including improving interagency coordination and obtaining sufficient information for decision making. Recently, agencies have taken several actions that may improve individual programs and processes in the export control system. However, the effectiveness of the existing system for protecting critical technologies depends on agencies working collectively. Our work in this area demonstrates the vulnerabilities and inefficiencies of the overall system. Consequently, we have called for the executive and legislative branches to conduct a fundamental reexamination of the current programs and processes, which remains to be done. This hearing will contribute to that reexamination.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or members of the subcommittee may have at this time.

GAO Contacts and Staff Acknowledgments

For further information about this testimony, please contact me at 202-512-4841 or lasowskia@gao.gov. John Neumann, Assistant Director; Jessica Bull; Jeff Hartnett; Steve Marchesani; Ramzi Nemo; and Karen Sloan made key contributions to this statement. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Related GAO Products

High-Risk Series: An Update. GAO-09-271. Washington, D.C.: January 2009.

Export Controls: Challenges with Commerce's Validated End-User Program May Limit Its Ability to Ensure That Semiconductor Equipment Exported to China Is Used as Intended. GAO-08-1095. Washington, D.C.: September 25, 2008.

Export Controls: State and Commerce Have Not Taken Basic Steps to Better Ensure U.S. Interests Are Protected. GAO-08-710T. Washington, D.C.: April 24, 2008.

Department of Defense: Observations on the National Industrial Security Program. GAO-08-695T. Washington, D.C.: April 16, 2008.

Foreign Investment: Laws and Policies Regulating Foreign Investment in 10 Countries. GAO-08-320. Washington, D.C.: February 28, 2008.

Defense Acquisitions: Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy. GAO-08-91. Washington, D.C.: January 11, 2008.

Defense Trade: State Department Needs to Conduct Assessments to Identify and Address Inefficiencies and Challenges in the Arms Export Process. GAO-08-89. Washington, D.C.: November 30, 2007.

Nonproliferation: U.S. Efforts to Combat Nuclear Networks Need Better Data on Proliferation Risks and Program Results. GAO-08-21. Washington, D.C.: October 31, 2007.

Defense Trade: Clarification and More Comprehensive Oversight of Export Exemptions Certified by DOD Are Needed. GAO-07-1103. Washington, D.C.: September 19, 2007.

Export Controls: Vulnerabilities and Inefficiencies Undermine System's Ability to Protect U.S. Interests. GAO-07-1135T. Washington, D.C.: July 26, 2007.

Defense Trade: National Security Reviews of Foreign Acquisitions of U.S. Companies Could Be Improved. GAO-07-661T. Washington, D.C.: March 23, 2007.

Export Controls: Challenges Exist in Enforcement of an Inherently Complex System. GAO-07-265. Washington, D.C.: December 20, 2006.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Mr. STUPAK. Thanks, Ms. Lasowski.

Mr. Borman, your opening statement, please.

TESTIMONY OF MATTHEW BORMAN

Mr. BORMAN. Thank you, Mr. Chairman.

Mr. STUPAK. We are going to need you to turn on a mike and pull it up there a little bit.

Mr. BORMAN. Thank you, Mr. Chairman——

Mr. STUPAK. Thank you.

Mr. BORMAN [continuing]. And members of the committee. We do appreciate, Tom Madigan and myself, the opportunity to come up here and talk to you about this. This is a very important topic, and we really appreciate your interest, the work of GAO, and industry interest. From our perspective this is an issue that really needs significant coordination between the Legislative Branch, the Executive Branch, and the U.S. private sector.

Just to give you a quick overview of our role in the system, of course, the U.S. Export Control System there is several different components. The dual-use system governs the export of items that have civilian and military applications and we administer at BIS the dual-use system in conjunction with a number of other agencies including the Departments of Defense, Energy, Homeland Security, Justice, State, and Treasury, as well as the intelligence community.

In administering the Dual-Use Export Control System BIS and other agencies develop control policies based on technologies, countries, end usages, and end users. While most items in the U.S. economy are subject to controls, that is, they are subject to the regulations, only a small percentage of U.S. exports by dollar value actually need a specific license from Commerce that goes through an interagency process.

And in administering the system we are very aware of the challenges of the 21st century, and the way we look at them is you have diffuse challenges; diffuse security threats ranging—there are a range of Nation States all the way down to non-State actors to individuals, but you also have a real diffusion of markets. When the Export Control System was first crafted, many of the major markets were not markets then, China and India being two obvious examples, and you have a much greater diffusion of technology. The U.S. is no longer the world leader in a range of technologies as it was say 20 years ago.

And our authorizing statute, which is the Export Administration Act of 1979, is a Cold War statute, and if anyone looks at it, you will see it replete with references to the Coordinating Committee for Multi-Lateral Export Controls. That was the trade equivalent to NATO that has ceased to exist in 1994. Not only is it the EAA 1979, it is in lapse. It is not permanent legislation, and in the years I have been in Commerce, I have been both in this position and our legal office for more than 15 years, it has only been in effect for about a year and a half total. So clearly there is a statute on the dual-use side that seriously needs revisions.

Pursuant to an executive order, we continue to apply the provisions of the act to the extent permitted by law and implement our regulations under another statute called the International Emergency Economic Powers Act or IEEPA. This authority provides for

a limited control over domestic transfers of items subject to the EAR that are deemed to be exports. That is in the technology area, technology to foreign nationals in the United States.

Consistent with our existing authority, we have outreach compliance and enforcement actions that address exports, re-exports, and foreign transfers, and these include certain domestic and third-country transfers of technology deemed to be exports or re-exports based on the involvement of foreign nationals.

Given the volume of trade from the United States, for example, it was about $1.3 trillion dollars worth of exports for the United States last year, informing U.S. and foreign businesses of the requirements of our regulations is a critical component to our Export Control System. We have a robust outreach program which includes seminars, web information, training, phone counseling, and direct preventative enforcement visits to companies. In addition to this outreach program we also have a broad compliance and enforcement program to help ensure that exports are in accord with the regulatory requirements.

Regarding compliance, we do things like following up with license reporting requirements, carefully reviewing data from the automated export system, which is the system exporters put their data in before trade leaves the country, and inform U.S. manufacturers, exporters, and shippers how to avoid becoming involved in potential export violations with various publications, including red-flag indicators, one of which specifically speaks to domestic transfers.

With that I will turn it over to my colleague who will address the enforcement aspects of our program. Thank you, Mr. Chairman.

[The prepared statement of Mr. Borman follows:]

Statement of

Matthew S. Borman

Acting Assistant Secretary for Export Administration,
Bureau of Industry and Security,
U.S. Department of Commerce

And

Thomas Madigan

Acting Deputy Assistant Secretary for Export Enforcement,
Bureau of Industry and Security,
U.S. Department of Commerce

before the

Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
United States House of Representatives

June 4, 2009

Chairman Stupak, Ranking Member Walden, and Distinguished Members of the Subcommittee:

We appreciate the opportunity to appear before the Subcommittee today to discuss the Bureau of Industry and Security's (BIS) role in administering and enforcing the U.S. dual-use export control system, a system focused on the shipment or transmission of items subject to the Export Administration Regulations (EAR) out of the United States and the reexport of such items from abroad.

Overview

The U.S. export control system has several different components. The dual-use system governs the export of items that have both civilian and military (weapons of mass destruction, conventional arms, terrorist) applications. BIS administers dual-use export controls by working closely with a number of other agencies, including the Departments of Defense, Energy, Homeland Security, Justice, State, and the Treasury, as well as the intelligence community. Other agencies are responsible for administering other parts of the U.S. export control system. The Department of State, for example, implements U.S. export controls on defense articles and services.

In administering dual-use export controls, BIS and other agencies develop control policies, based on technologies, countries, end-uses, and end-users. These policies are set forth in the EAR.

The regulations specify what types of items (commodities, software, technology) are subject to control. The EAR controls two types of items – those enumerated on the Commerce Control List and most other items, which are designated by a basket category (EAR99).

Although the EAR's coverage is broad, only a small percentage of U.S. exports, by dollar value, are exported under a Commerce license. In 2008, for example, of the $1.3 trillion worth of exports from the United States, only $3.1 billion was exported under a Commerce license.

The EAR's authorizing statute, the Export Administration Act (EAA), has been in lapse since 2001. However, the EAA and EAR are maintained, to the extent permitted by law, through an executive order issued pursuant to the International Emergency Economic Powers Act (IEEPA). Pursuant to the EAA, IEEPA, and the EAR, BIS administers controls over exports, reexports, and domestic transfers of technology and source code ("deemed exports") subject to the EAR. Accordingly, BIS's outreach, compliance, and enforcement efforts address exports, reexports, and certain domestic transactions where parties involved have knowledge that the item will be or has been subsequently exported.

Outreach

Given the volume of trade from the United States, informing U.S. and foreign businesses of the requirements of the EAR is a critical component of our dual-use export control system. BIS, through counseling offices in Washington, DC and California, provides extensive export control assistance to the business community. These educational outreach activities help facilitate industry compliance through individualized counseling sessions and outreach training programs.

In 2008, BIS provided one-on-one counseling to over 55,000 individuals and conducted 36 seminars in 16 states. The seminars covered basic export control principles, controls on technology and encryption, and developing and enhancing industry compliance programs. Further, BIS provided export control information in 38 trade events sponsored by other organizations.

In addition, BIS's export enforcement arm conducts even more specialized outreach. These "preventive enforcement" efforts involve direct outreach to manufacturers, exporters, shippers, freight forwarders and other members of the exporting community to educate them on export control requirements, encourage voluntary compliance, and detect potential violations. This is performed in order to ensure that due diligence is applied when determining the end-use, end-user, and destination of proposed exports. In addition to educating industry, our intention is to elicit its cooperation in protecting U.S. national security and foreign policy objectives.

Outreach allows for better communication between government and industry, and directly assists enforcement investigations and operations.

Compliance

BIS does not, however, rely solely on outreach to help ensure exports are undertaken in accordance with the requirements of the EAR. BIS also has a broad compliance and enforcement program.

BIS conducts comprehensive reviews of all licenses with reporting requirements. License reports are analyzed by our compliance specialists for completeness and timeliness, and licensees are contacted if additional information is required. Any circumstances related to the license condition reports that indicate potential violations or non-compliance are referred for further enforcement follow-up.

BIS also carefully reviews data on exports in the Automated Export System (AES). Comparing license and shipment data on a monthly basis, BIS evaluates whether items subject to a license requirement are exported in accordance with the EAR. BIS has instituted electronic validations in AES to preemptively identify problematic transactions and bolster exporter compliance.

Over the past year, we have increased exporter compliance with the AES filing requirements in the EAR by 11%, and currently 96% of exports subject to the EAR are compliant. For those non-compliant transactions, BIS uses targeted outreach and enforcement authorities to remedy deficiencies. We are also continuing to work with the Census Bureau and Customs and Border Protection to further enhance the capabilities of AES to flag additional transactions that may trigger compliance concerns.

BIS recognizes that U.S. manufacturers, exporters and shippers are in an excellent position to spot potential illegal export activity. They may well be the first parties contacted by potential violators of the EAR, such as weapons of mass destruction proliferators, terrorist support organizations, and illicit procurement networks/front companies trying to acquire U.S.-origin dual-use items. BIS has published guidelines to help U.S. manufacturers, exporters and shippers avoid becoming involved in potential export violations. These guidelines are known as the Know Your Customer guidance and Red Flag Indicators.

Informed, voluntary compliance with U.S. export controls by the export trade community is a key component of BIS's export administration and enforcement programs. All parties to U.S. export transactions must ensure that their exports fully comply with all statutory and regulatory requirements. Compliance not only involves controlled goods and technologies, but also restrictions on shipping to certain countries, companies, organizations, and/or individuals.

While there is no explicit requirement in the EAR for domestic sellers to screen their customers, many companies do as a matter of due diligence because of potential liability. Companies are aware of this potential liability, as BIS works closely with the export trade community to raise awareness of compliance best practices and "red flags" of potential illicit export activities, and to identify and act on export violations. BIS's "red flag" guidance focuses on how individuals and firms should take into account any abnormal circumstances in a transaction that indicate that the transaction may be destined for an inappropriate end-use, end-user, or destination.

In fact, one "red flag" indicator specifically points to domestic transactions involving potential exports. That indicator states: "When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for reexport." These indicators are published in the EAR, posted on the BIS website, included in BIS training material and publications, and routinely discussed at BIS's export control seminars, in one-on-one counseling and during targeted outreach with industry.

BIS is also part of the Commerce team that supports the interagency Committee on Foreign Investment in the United States (CFIUS), which reviews transactions that could result in control of a U.S. business by a foreign person in order to determine the effect of such transactions on the national security of the United States. BIS evaluates CFIUS transactions to identify issues with regard to dual-use export controls and the defense industrial base. The reviews also provide an avenue for identifying producers of controlled products who may not export, and thus be less aware of EAR requirements.

Enforcement

BIS's mission is designed to keep sensitive U.S. dual-use goods and technology from being diverted to proscribed end-users, end-uses, and destinations. Enforcement priorities include conducting investigations that target: weapons of mass destruction proliferation; terrorism and state sponsors of terror; and the unauthorized military end-use of items consistent with BIS's mandate to regulate exports of items with both civilian and military applications. To identify and investigate potential and actual violations of dual-use items under the EAR, BIS's export enforcement arm has approximately 80 assigned special agents in many regions of the United States and stationed abroad, and another 43 supporting analysts and other staff.

BIS Special Agents use the Automated Targeting System (ATS) portion of the AES database to identify violators in the United States and overseas. On a daily basis, Special Agents check the ATS database for shipments destined to embargoed or sanctioned countries, such as Iran or Syria. Quite often, these shipments are detained before reaching their destination, preventing an unauthorized shipment from reaching those countries. In addition, Special Agents conduct reviews in ATS and compare the results against sanctioned parties on the BIS Entity List and Denied Persons List.

There are numerous examples of how this process has caught shipments destined to prohibited parties and destinations. It can lead to identification of other overseas diverters as well. If BIS or another government agency identifies a diverter overseas, ATS searches can be completed to identify unwitting suppliers to these diverters. Violations can be prevented by advising these exporters that their products may ultimately be diverted in violation of the EAR. Similarly, this also sometimes leads Special Agents to complicit U.S. diverters that are prosecuted.

BIS also investigates procurement networks that employ various types of diversions in order to acquire sensitive U.S. dual-use goods and technology for end-users and end-uses contrary to the national interests of the United States. In addressing the threat of dual-use diversion, BIS encounters circumstances in which foreign parties have attempted to secure what appears to be a 'domestic order' but which in fact is intended for export to either end-users or end-uses in a

transaction that would not otherwise receive a license from BIS. Due to its targeted outreach, BIS identifies such attempts and is able to investigate, interdict, and prosecute with partner agencies.

A recent example involved the disruption of an illicit procurement network acquiring controlled thermal imaging (i.e., night vision) cameras for delivery to the People's Republic of China (PRC). After receiving an industry tip and conducting a thorough investigation and "controlled delivery", the suspects were arrested while boarding a flight to the PRC. Ten thermal imaging cameras found concealed in their luggage were interdicted prior to being illegally exported from the United States. Interdiction of the cameras prevented their potential use by unauthorized end-users to operate under low-light conditions. Due to BIS's industry outreach program, Special Agents were able to disrupt this unlawful procurement attempt through surveillance, searches, interviews, document review, and evidence and witness preparation. One defendant pled guilty to the charges against him and cooperated in the trial convicting his co-conspirator. Information gathered during this investigation is being used by federal law enforcement agencies targeting illicit procurement efforts.

The Administration is reviewing the existing law enforcement authorities of BIS Special Agents to determine if additional authorities are needed to enable BIS to better address the current security and commercial environment.

Conclusion

We appreciate the opportunity to testify in front of the subcommittee regarding our important national security mission. In addition to the timely and rigorous review of license applications, an effective export control system requires a combination of domestic and international activities to educate parties on their export control responsibilities, proactive compliance efforts, and the conduct of enforcement investigations. Our dedicated staff, with support from many other agencies, is committed to protecting U.S. national security, foreign policy, and economic interests by ensuring secure trade in high technology items.

We would be pleased to answer any questions you have.

Mr. STUPAK. Thank you, Mr. Borman.
Mr. Madigan.

TESTIMONY OF THOMAS MADIGAN

Mr. MADIGAN. Thank you, Mr. Chairman.
Mr. STUPAK. Do you want to share that mike there? There we go.
Mr. MADIGAN. Excuse me. Thank you, Mr. Chairman, Ranking Member Walden, and distinguished members of the subcommittee. As a follow up to Mr. Borman's comments on BIS outreach efforts, I would only add that BIS's export enforcement arm conducts additional targeted specialized outreach visits. These preventive enforcement efforts involve direct outreach to members of the exporting committee, community to educate them on export control requirements, to encourage voluntary compliance, and to detect potential violations. Over the past year we have conducted over 3,400 such targeted outreach visits.

BIS's mission of keeping U.S. dual-use goods and technology from being diverted to prescribed end users and end uses is an important one. Our enforcement priorities include weapons of mass destruction, proliferation, terrorism, and State sponsors of terror, and unauthorized military end use of such items. To further this mission we have special agents assigned to eight regional field offices across the U.S. and in five foreign locations supported by administrative staff of analysts and other employees.

With respect to AES, which Matt mentioned, BIS special agents use the automated targeting system of AES to identify violators in the United States and overseas. ATS queries can be conducted to identify unwitting suppliers to foreign diverters. Violations can then be prevented by advising these exporters through this targeted outreach that their products may ultimately be diverted in violation of the EAR.

In addressing the threat of dual-use diversion by foreign procurement networks, BIS sometimes encounters circumstances in which foreign parties have attempted to secure what appears to be a domestic order but which is, in fact, intended for export. During its targeted outreach BIS has identified such attempts in the past and has investigated and prosecuted the suspects with its partner agencies.

A recent example of this included the disruption of the network attempting to control—to acquire controlled thermal imaging cameras for export to the PRC. After receiving an industry tip and conducting a thorough investigation, the suspects were arrested while boarding a flight to Beijing with ten of the controlled cameras concealed in their luggage. Due to the successful outreach in this case, agents were able to interdict the goods, disrupt the domestic procurement attempt, and prosecute the individuals involved.

We greatly appreciate the opportunity to testify in front of the committee today, subcommittee today, regarding BIS's important national security mission. Our dedicated staff, with support from many other agencies, is committed to protecting our national security, foreign policy, and economic interests by ensuring secure trade in high-technology items, so we welcome this discussion.

We would be pleased to answer any questions you may have.
Mr. STUPAK. Thank you, Mr. Madigan.

Mr. Alvis, your opening statement, please, sir, and pull that mike up and you got to hit the button there. It should turn on a green light, and you'll be all set there. Pull that up there a little bit. Thanks.

TESTIMONY OF MICHAEL ALVIS

Mr. ALVIS. Good morning. Chairman Stupak, Ranking Member Walden, members of the committee. My name is Mike Alvis, and I am a Vice President at ITT Night Vision, a $500 million business within the ITT Corporation, Fortune 500 corporation with over 40,000 employees worldwide. Our products serve a broad range of applications in both military and commercial markets. They include products like pumps for residential and commercial water, imagers on weather satellites, and the ground station network for the next generation U.S. air traffic control system.

I am joined at the hearing today by Mr. Gregg Nivala, ITT's general counsel and the head of our trade compliance organization. His organization monitors all—the sale of all products, military and commercial. Also in attendance today is Mrs.—Ms. Ann Davidson, Corporate Vice President at our world headquarters, and she serves as ITT's Vice President for Corporate Responsibility. Also in attendance is Mr. Doc Syres, our Vice President for Congressional Relations.

ITT has been in the night-vision business for 50 years. We are pleased to make ourselves available to this committee as it investigates the sale of sensitive military technology into the commercial marketplace. In the interest of full disclosure, in early 2007, ITT settled a criminal matter with the U.S. Department of Justice by pleading guilty to violations of the International Traffic and Arms Control Regulations or ITAR. The individuals joining me here today hold key positions created as a result of that settlement, and they serve at the corporate and business unit level that is designed to ensure that all ITT employees know and understand the law and operate their business activities legally and ethically.

Ms. Davidson is the first ever Vice President for Corporate Responsibility and presides over a worldwide network of compliance officials that monitor the business units to ensure that ITT moves forward with a premiere ethics and compliance program.

ITT Night Vision where I work is the world's largest developer and manufacturer of night-vision goggles and image-intense fire tubes for other systems. We are only one of two manufacturers of the Generation 3 image tubes. Both companies happen to be U.S. This is the technology of the goggle.

We began making these tubes in 1982, and have manufactured over a million Gen 3 tubes, and we have ceased manufacturing the Generation 2 tubes, which many of you see in the commercial marketplace and in catalogs. Our key domestic business areas are night-vision goggles and spare tube sales to U.S. and Federal Government agencies and State and local first responders. ITT also sells its Generation 3 aviation goggles to the civil helicopter community, primarily emergency medical services.

Although not a governmental entity, private medical evacuation helicopters perform a key first responder role, and the use of night-vision goggles in their operations is recommended by the Federal

Aviation Administration. ITT is currently in the process of doubling the number of goggles available to the civil aviation community for Medi-Vac.

Less than 1.5 percent of our sales are to commercial end users, and 85 percent of those sales are to the civil helicopter community I just referred to. The other .04 percent of our business, the remaining 15 percent, go to the—into the commercial market, but it should be noted that ITT does not provide military specification tubes for those sales. They go to people like ranchers, nature lovers, and other recreational users. We call these fall-out tubes. These are the scrap that come out of our process and as—and they have some value commercially.

ITT is also the developer and sole provider of the enhanced night-vision goggle, the most versatile and multi-faceted night-vision device ever fielded. The ENVG and its special 16 millimeter tube is only sold to the United States Army, and this views also in special operations. It will continue to ensure that U.S. forces always have the critical technological edge or overmatch over potential adversaries.

In closing, ITT is pleased to answer your questions today concerning our technology and our experience in developing a first-class trade compliance organization, consistent with the requirements set forth in the ITAR. We will limit our responses to questions concerning night-vision technology that are in the public domain. We look forward to your questions.

[The prepared statement of Mr. Alvis follows:]

ITT Corporation

CONGRESSIONAL TESTIMONY

STATEMENT OF ITT CORPORATION

Testimony before

The Subcommittee on Oversight and Investigations

Committee on Energy and Commerce

United States House of Representatives

Mike Alvis

Vice President, Strategy and Business Development
ITT Night Vision

and

Gregg Nivala

Vice President, General Counsel
and Director, Trade Compliance
ITT Night Vision

June 4, 2009

Chairman Stupak, Ranking Member Walden and members of the Committee.

My name is Mike Alvis, I am a Vice President at ITT Night Vision--one of the seven businesses in the ITT Defense Electronics and Services Group within ITT Corporation, a multi-national, multi-industry Fortune 500 corporation with over 40,000 employees and $10 billion dollars in annual revenue. Our products serve a broad range of applications in both military and commercial markets. They include things like pumps for the residential and commercial water market, sounders and imagers on weather satellites which will help us measure the impact of carbon in our atmosphere, and the ground station network for ADS-B which will transform the FAA's air traffic control function from its sole reliance on radar to include more precise GPS satellite technology.

I am joined at the witness table today by Mr. Gregg Nivala, ITT Night Vision's General Counsel. Gregg also heads the ITT Night Vision trade compliance organization that monitors the sale of all of our products, military and commercial. Also in attendance is Ms. Ann Davidson, from our corporate headquarters. She serves as ITT's Vice President for Corporate Responsibility.

ITT has been in the night vision business for over 50 years. We are pleased to be an informational resource for this Committee as it investigates the sale of sensitive military technology into the commercial marketplace. In the interest of full disclosure, in early 2007, ITT settled a criminal matter with the US Department of Justice by pleading guilty to violations of the International Traffic and Arms Control Regulations or ITAR. The individuals joining me here today hold key positions created at the corporate and business unit level designed to ensure that all ITT employees know the law and operate their business activities legally and ethically. Ms. Davidson, the first ever corporate Vice President for Corporate Responsibility, presides over a worldwide network of compliance officials that monitor the business units to ensure that ITT moves ever forward with a world class or premier ethics and compliance organization.

ITT Night Vision is the world's largest developer and manufacturer of night vision goggles and image intensifier tubes for weapons sights, aerial

platforms and other specialty systems manufactured by other US companies. We are one of only two US manufacturers of the Generation 3 (Gen 3) image tubes, the highest technology developed to date. It is the core component for US military night vision goggles. Since 1982, ITT has manufactured over one million Gen 3 tubes. ITT's night vision value center employs over 1,900 people in two locations in Virginia and Massachusetts and earns about $500 million in annual revenues. The overwhelming preponderance of our sales is to government customers and we have ceased manufacturing Generation 2 tubes which often constitute the technology found in catalog commercial sales for the public. Our key business areas are night vision goggle and spare tube sales to US federal agencies and state and local governments, international sales to key US allies, and commercial tube sales to other US original equipment manufacturers (OEM) who sell into the US military market. ITT also sells its Gen 3 aviation goggles—via a dealer—to the civil helicopter community--primarily emergency medical services (EMS). Although not a government entity, private medical evacuation helicopters perform a key first responder role and the purchase and use of night vision goggles by them is strongly encouraged by the Federal Aviation Administration.

Until recently, ITT's focus was image intensification technology which involves the magnification of small amounts of ambient light through processing plates that excite protons and produce visible images against a green backdrop. ITT is also the developer and sole provider of the Enhanced Night Vision Goggle (ENVG), the most versatile and multifaceted night vision device ever fielded. This goggle uses an optical fusion to overlay a Gen 3 tube with a thermal infrared image giving the soldier multiple viewing modes and operability in all battle and environmental conditions. The ENVG is only sold to the US Army. It should continue to ensure that US forces always have the critical technological edge over potential adversaries. This overmatch is also maintained in the international sales of legacy Gen 3 products by enforcing US government restrictions on the specification of Gen 3 tube allowed to be sold internationally. This applies even to our closet allies. In addition to limiting the quality of the overall tube characteristics, recent "provisos" from the Department of State and Department of Defense maintain the US advantage by not allowing "gated" tubes to be sold even to our closest Allies. The gated feature allows a tube to continue to function when there is a sudden increase in light, such as during a firefight. Non-gated tubes would shut down for a period because they are overwhelmed by the increase in light. As a matter of policy, ITT

does not sell its Pinnacle gated image intensifier tube into the US commercial market. The two exceptions are the civil aviation and law enforcement markets where its safety and operational overmatch are essential ingredients to mission success.

Given this committee's interest and focus, it is important to understand the distinction between the Gen 3 technology and the Gen 2 technology that is available from multiple international manufacturers located in Russia, France and the Netherlands. This is important because currently there are no restrictions on the import of Gen 2 tubes into the US. Gen 2 tubes are the main component in the US recreational market and even contribute to some US military and law enforcement sales. The Gen 2 tubes produced abroad have improved and equal or surpass the Gen 3 tubes in some areas. The "Gen 2 Plus" currently produced by Photonis-DEP, a French-Dutch company, performs superbly at most levels of the night spectrum and competes favorably with ITT and L-3 Communications in the international market.

The Gen 3 tube, the only tube manufactured by ITT, outperforms the Gen 2 Plus in three major areas (only one of them electro optical): low light level performance, life cycle costs and initial costs. The US military prefers to operate at night at the lowest level of ambient light available. This helps ensure that they always have the advantage over an adversary with the naked eye or Gen 2 technology. The superior low light level of Gen 3 over Gen 2 gives the US a qualitative edge when little light is available. In areas where ambient light is prevalent, such as urban areas, the advantage diminishes. The other advantage of Gen 3 is that the tube lasts four times as long, reducing the logistical burden on the US military which will have one million goggles deployed throughout the world by the end of 2010. Finally, the ITT Gen 3 tubes are cheaper due to ITT's high volume supply chain, lean and Six Sigma efficiencies and high yields.

In closing, ITT is pleased to answer any questions concerning our technology or our experience in developing a first-class compliance organization to protect this technology and all ITT products and services of a sensitive nature. Consistent with the requirements set forth in the International Traffic and Arms Regulations (ITAR), we will limit our responses to questions concerning Night Vision technology to information that is in the public domain.

While ITT is the world's leading manufacturer of Gen 3 image intensification tubes, we do not make all the individual systems that are bought and used by the US military. Specialty items like weapons sights, aerial cameras, and Special Operations equipment are made by smaller companies who specialize in that market. ITT sells its Gen 3 tubes to those original equipment manufacturers as a commercial sale. We hope that the Committee will very carefully examine the balance between increasing regulatory protection and an overly restrictive prohibition on commercial sales. Prohibiting direct commercial domestic sales of night vision tubes could impact our military and the small companies that support them. It also could adversely impact medevac helicopters. We look forward to your questions.

Mr. STUPAK. Thank you.
Mr. Roush, your opening statement, please.

TESTIMONY OF JOHN ROUSH

Mr. ROUSH. Good morning, Chairman Stupak——
Mr. STUPAK. You might—you got that mike on?
Mr. ROUSH [continuing]. Other members of the committee. Thank you for the opportunity to participate in today's hearing. My name is John Roush, and I am a Senior Vice President at Perkin Elmer and President of the company's environmental health business segment.

Perkin Elmer has a 60-year history of innovation in life sciences, analytical instrumentation, and optoelectronics products. We are a global leader focused on improving the health and safety of people and the environment. We are headquartered in Massachusetts and have about 8,500 employees serving customers in more than 150 countries. We have significant U.S. operations in six different States. In 2008, we reported revenue of approximately $2 billion, and we are proud to be a component of the S & P 500 index.

As discussed, today's hearing will review the U.S. Government's safeguards in place to prevent the unauthorized diversion of sensitive products by a domestic purchase. Let me say that Perkin Elmer is committed to help solve this problem in various ways as discussed by Representatives Walden, Markey, and other members of the committee.

As you know, the Department of Commerce and the Department of State are responsible to export control regulations within their respective jurisdiction. Let me tell you that Perkin Elmer takes these requirements very seriously. As part of our commitment, we have implemented an export management system to ensure that we are complying with all applicable U.S. export control laws. Our system establishes a robust internal compliance capability to prevent the transfer of sensitive or controlled products for improper end uses or to unauthorized destinations or purchasers.

Additionally, our compliance processes incorporate the know your customer and red-flag indicators' guidelines issued by the U.S. Government. We have a staff of dedicated export control compliance personnel who are regularly trained on U.S. export control requirements and who play an integral role in the sale of these controlled products.

Let me tell you that Perkin Elmer's export compliance program is very effective. In fact, we have been viewed a model within our industry by various compliance agencies that we have dealt with in the past. As mentioned by Representative Markey, of particular interest to this committee Perkin Elmer has also shown a track record of cooperating with government agencies in export compliance matters.

In 2003, Perkin Elmer alerted representatives of BIS's Office of Export Enforcement of a request we had received to purchase 200 triggered spark gaps for shipment abroad. Perkin Elmer followed its established internal screening procedures and identified several red flags. In this transaction the number of items in the order quantity was inconsistent with the stated medical purpose in that

region of the world, and the proposed sale lacked appropriate export documentation.

In this case Perkin Elmer worked closely with OEE and other federal agencies in a sting operation involving a New Jersey customer to track the ultimate destination for those goods, which was Pakistan. The individual who attempted to arrange this transaction was convicted of violating U.S. export control laws and received a 3-year prison sentence. We are proud that the U.S. authorities publicly acknowledged Perkin Elmer for its role in this investigation.

I want to say that Perkin Elmer is fully committed to compliance with all applicable U.S. laws. We commend this committee and other interested stakeholders for your interest in considering possible ways to enhance U.S. Government safeguards for domestic sales of certain sensitive products. We stand ready to support the committee's efforts.

We do hope that such reforms will not disrupt the ability of domestic buyers to purchase these products for critical and legitimate medical needs. We look forward to working with you to ensure that any such proposals are effective and can be implemented in a reasonable manner. We thank you for the opportunity to make this statement, and I will be happy to take your questions at the appropriate time.

[The prepared statement of Mr. Roush follows:]

Testimony of John Roush,
Senior Vice President and President of Environmental Health of PerkinElmer, Inc.

Before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations

June 4, 2009

Good morning Subcommittee Chairman Stupak, Ranking Member Walden and other Members of the Committee. Thank you for the opportunity to participate in today's hearing on the commercial sale of certain sensitive technologies.

My name is John Roush, and I am a senior vice president of PerkinElmer, Inc. ("PerkinElmer") and president of the Company's Environmental Health business.

* * *

PerkinElmer has a sixty-year history of innovation in life sciences, analytical instrumentation and optoelectronics. This history originates from the combination of a company founded by three MIT professors, who joined to study the mechanisms and applications of high-speed photographic and stroboscopic techniques, and The Perkin-Elmer Company, which was then an optics design and consulting business. Today PerkinElmer is a global leader focused on improving the health and safety of people and the environment. PerkinElmer is headquartered in Waltham, Massachusetts, and has about 8,500 employees serving customers in more than 150 countries, with significant U.S. operations in Massachusetts, Pennsylvania, Ohio, California, Connecticut and Illinois. In 2008, we reported revenue of approximately $2 billion, and we are proud to be a component of the S&P 500 Index.

* * *

Our understanding is that today's hearing will review U.S. government safeguards in place to prevent the unauthorized diversion of sensitive products. As you know, the Department of Commerce and the Department of State are responsible for export control regulations within their respective jurisdictions. PerkinElmer takes these requirements very seriously. As part of its commitment, PerkinElmer has implemented an "Export Management System ("EMS") Manual," which provides effective guidance and procedures to ensure that we are complying with all applicable U.S. export control laws. Our EMS and supporting Standard Operating Procedures (SOPs) establish a robust internal compliance capability to prevent the transfer of sensitive or controlled products to unauthorized destinations, persons or entities, including those named on any of the restricted party lists, or to improper end-uses, including activities related to weapons of mass destruction and proliferation. Additionally, our compliance processes

incorporate the "Know Your Customer" and "Red Flag Indicators" guidelines issued by the U.S. Department of Commerce, Bureau of Industry and Security ("BIS"), and we have dedicated export compliance personnel who are regularly trained on U.S. export control requirements and who play an integral role in our processing of orders for these kinds of products and technologies.

* * *

PerkinElmer's export compliance program works effectively. Of particular interest to this Committee, PerkinElmer also has a proven track record of cooperating with government agencies in export compliance matters. In 2003, for instance, PerkinElmer alerted representatives of BIS's Office of Export Enforcement ("OEE") of a request to purchase 200 triggered spark gaps for shipment abroad. PerkinElmer followed its established internal screening procedures and identified certain "red flags." Specifically, the proposed sale lacked appropriate export documentation, and the number of items in the order was inconsistent with its stated medical purpose. In this case, PerkinElmer worked closely with OEE, and other federal agencies, to facilitate the sale of these items (which had been disabled prior to shipment) and to track their ultimate destination, which was Pakistan. The individual who had attempted to arrange this transaction was ultimately convicted of violating U.S. export control laws and received a three-year prison sentence. We are proud that the U.S. authorities commended PerkinElmer for its role in the investigation.

We understand that the Committee may have questions about triggered spark gaps. For those of you who do not know, triggered spark gaps are a family of versatile high voltage switches that consist of three electrodes in a hermetically sealed, pressurized ceramic envelope that have important medical uses. For example, we make spark gaps for medical lithotripter applications, including the fragmentation and disintegration of kidney stones. Typical purchasers of this spark gap include medical device manufacturers and companies that service hospital equipment. We understand that a single sample triggered spark gap was purchased from PerkinElmer by a domestic front company established by the GAO, and we handled this transaction using our established screening process for purchases of this product by a domestic customer.

* * *

PerkinElmer is fully committed to compliance with all applicable U.S. laws. We commend the Committee and other interested stakeholders for your interest in considering possible ways to enhance U.S. government safeguards for domestic sales of certain sensitive products. We stand ready to support the Committee's efforts to prevent certain sensitive products from being diverted for unlawful purposes or end-users, but hope that such reforms will not disrupt the ability of domestic buyers to purchase and deploy those products for critical

medical needs. We look forward to working with the Committee and other interested stakeholders to ensure that any such proposals are effective and can be implemented in a reasonable manner to the extent that they require the support of businesses such as ours. Thank you for the opportunity to make this statement, and I will be happy to take any questions you might have.

Mr. STUPAK. Thank you.
Mr. Fitton, your opening statement, please, sir.

TESTIMONY OF NICHOLAS FITTON

Mr. FITTON. Honorable Chairman and members of the committee, I am Nicholas Fitton, sole owner and operator of a small store located in Georgia Section 8. I am here today because of the sale of an F110–GE–129 engine computer. This is an item which is restricted from export. Other than that there are no restrictions placed on the sale of this item.

When I purchased it in 2006, from Government Liquidations, the institute which controls the sale of auction surplus, government military items, I filed paperwork stating it was for resale. The customer was unknown at that time, and that it would not be exported or altered in any way.

In December of 2008, I was contacted by a person identifying himself as Joseph Fitzpatrick, wished to have more information on the item. After several contacts the individual placed an order on January 20, 2009. You have in your possession copies of all correspondence between the purchaser and myself, along with my inter-office file on the transaction.

After the order was placed, I had the individual fill out an end-use certificate and send a copy of identification along with the application to my office. Unfortunately as a seller I do not actually have access to background checks and certificates that I could submit to a government agency such as Government Liquidations does. The end-use certificate I had the customer fill out is one that I copied and edited from their Web site. After I received the customer's information I obtained satellite imagery of the street address the buyer's home address was listed as and did the same for his place of business. The imagery verified they were residential and business districts. I also pulled public information on the company the buyer had listed, all information include IP addresses of the computer the transactions were placed from is maintained both in digital and hard-copy formats.

I also called in a favor from a local law enforcement officer who just simply ran the buyer's name through a computer to see if there were any wants or warrants. Pretty much this is all that I can do as a seller.

During the process I had the buyer believe a more complex investigation was taking place than there actually really was. I also drew the process out over a long period of time. My experience in law enforcement military operations has shown that the longer transactions take and more security measures that are presented to an individual, if they are committing nefarious or criminal activities, they tend to become nervous and back out of the transactions or tend to give tells as to something is going wrong. The entire process from initial contact until the package was shipped on April 23 was over 4 months. A short time after the package was delivered, I was contracted by your investigators in regards to the matter, and here we are today.

What we are really looking at here has several issues which need to be addressed. One, formal guidelines need to be set for as to what is expected from resellers and end users, and this needs to

be something other than no exports as we have already talked about here.

Two, resources need to be opened up to resellers to which they can validate an end user. There are currently no such services available to vendors who sell materials deemed sensitive. Other industries such as firearms dealers have services available to them such as those offered by the Bureau of Alcohol, Tobacco, and Firearms, which will allow sellers to perform checks and investigations into those wishing to purchase these items. Government Liquidations has such services available and any vendor or person wishing to purchase these items has to be checked prior to them being able to pick up these items. Once it falls into the hands of the vendor or end user, the only requirement is not to export the item unless prior approval is granted.

The demilitarization codes is my third issue which needs to be addressed. Right now the demilitarization codes are fairly broad. For example, a piece of cloth is considered a restricted item because it is used as covering for a piece of armor or a helmet and thus classified in the same manner as body armor. A shirt or jacket which is 40 years old and hasn't been issued in years is classified the same way current issue items are.

And on that note we need to look at why certain items are classified as sensitive and no longer offered for sale. Many of these items while being available directly from manufacturers without restrictions are sold new across the country. Why is that same item being used by the military and in many cases, no longer serviceable, classified as sensitive?

Also, many items which do have restrictions such as armor, more specifically helmets, are now no longer available for sale. These items were once available with approval by an end-use certificate. While many people don't understand why someone would want or need one of these, they fail to realize that the primary consumer for such items tend to be law enforcement agencies. Many departments only have the budget to purchase tactical equipment including ballistic shields and helmets for their swat or quick reaction teams. They cannot afford four or $500 for a helmet for every patrol officer, even realizing the first responder to a hostile situation such as an active shooter is not a tactical unit but actually patrol officers. These surplus military helmets can be normally sold for under $50.

By restricting items for sale and commercial trade, not only are you taking away items from average citizen, but in many cases you are also affecting law enforcement as well. Even with policies such ammunition and weapons restrictions to civilians, law enforcement and even our military are adversely affected. This could be seen in the 1994, assault weapons ban and its subsequent sunset. After the ban was lifted more companies were able to afford research and development and quickly improve long-standing, stagnant technologies and simultaneously improve quality and lower the price of items used by military and law enforcement agencies.

With continued heavy taxation and uncoming restrictions, I am afraid it will not take much to make us rely on foreign powers for our military and law enforcement needs.

In conclusion, what we are dealing here with is not an inability to enforce security measures, but a lack of policy and procedures to enforce and lack of using commonsense to understand what the actual items are that are being sold. I currently have a bag with several types of simple cloth items which are current regulations considered more sensitive than many of the items up there on display. I have no restrictions as to what I can do with those items, however, a piece of cloth is required for me to be returned to the government for destruction.

At this time I open myself up for any questions in regards to these matters. Thank you.

[The prepared statement of Mr. Fitton follows:]

Testimony of Nicholas Fitton
Section 8

Honorable Chairman and members of the Committee…

I am here today because of the sale of an F110-GE-129 engine computer. This is an item which is restricted from export. Other than that, there are no restrictions placed on the sale of this item. When I purchased this item in 2006 from Government Liquidations, the entity which is used to auction surplus government and military items, I filed paperwork stating that it was for resale, the customer was unknown at that time and that it would not be exported or altered in any way. In December of 2008, I was contacted by a person identifying himself as Joseph Fitzpatrick. He wished to have more information on this item. After several contacts, the individual placed an order on January 20th, 2009. You have in your possession copies of all correspondence between the purchaser and myself, along with my interoffice file of the transaction. After the order was placed, I had the individual fill out an end use certificate and send a copy of identification along with the application to my office. Unfortunately, as a seller, I do not actually have access to background checks and certificates that I can submit to a government agency such as Government Liquidations does. The end use certificate I had the customer fill out is one that I copied and edited from Government Liquidations' website. After I received the customer's information, I obtained satellite imagery of the street address the buyer's home address was listed as and did the same for his place of business. This imagery verified that they were residential and business districts. I also pulled public information on the company the buyer had listed. All information, including IP addresses of the computer the transaction is placed from, is maintained in both digital and hardcopy formats. I also called in a favor from a local law enforcement officer who ran the buyer's name through the computer system to see if there were any wants or warrants. During this process, I had the buyer believe that a more complex investigation was taking place than actually was. I also drew the process out over a period of time. My experience in military and law enforcement has shown that the longer transactions take and the more security measures that are presented cause individuals who are conducting nefarious and criminal activities to become nervous and either back out of transactions or begin to give "tells" that something is wrong. The entire process from initial contact (December 17th, 2008) until the package was shipped on April 23, 2009 was over 4 months. A short time after the package was delivered, I was contacted by your investigators in regards to this matter. And here we are today…

What we are looking at has several issues which need to be addressed:

1. Formal guidelines need to be set as to what is expected from resellers and end-users. This needs to be something other than "no exports".
2. Resources need to be opened up to resellers through which they can validate an end-user. There are currently no services available to venders who sell materials deemed "sensitive". Other industries, such as firearms dealers, have services available such as those offered by the Bureau of Alcohol, Tobacco, and Firearms, which will allow sellers to perform checks and investigations into those wishing

to purchase these items. Government Liquidations has such services available and any vendor or person wishing to purchase these items must be checked prior to being able to pick up the items. Once it falls into the hands of the vendor or end-user, the only requirement is to not export the item unless prior approval is granted.

3. The demilitarization codes of items need to be re-addressed and not as broad. For example, a piece of cloth is considered a restricted item because it is used as a covering for a piece of armor or a helmet and thus is classified in the same manner as armor. A shirt or jacket which is 40 years old and hasn't been issued in years is classified the same way current issue items are. And on that note, we need to look at why certain items are classified as sensitive and no longer offered for sale. Many of these items are available directly from the manufacturers without restriction and are sold as new across the country. Why is that same item, if having been used by the military and in many cases no longer serviceable, classified as sensitive? Also, many items which do have restrictions, such as armor, more specifically, helmets, now are no longer available for sale. These items were once available, after approval, by an end use certificate. While many people don't understand why someone would want or need one of these, they fail to realize that the primary consumer for items such as these tend to be law enforcement agencies. Many departments only have the budget to purchase tactical equipment including ballistic shields and helmets for their swat or quick reaction teams. They cannot afford $400-$500 for a helmet for every patrol officer, even after realizing that the first responder to a hostile situation such as an active shooter is not a tactical unit, but actually are patrol officers. These surplus military helmets can be sold normally for under $50. By restricting items for commercial trade, not only are you taking items away from average citizen, but in many cases you are also affecting law enforcement as well. Even with policies such as ammunition and weapon restrictions to civilians, law enforcement and even our military are adversely affected. This can be seen in the 1994 assault weapons ban and its subsequent sunset. After the ban was lifted, more companies were able to afford research and development and quickly improve long standing stagnant technologies and simultaneously improve quality and lower the price of items used by military and law enforcement agencies. With continued heavy taxation and upcoming restrictions, I am afraid that it will not take much to make us reliant on foreign powers for our military and law enforcement needs.
4. In order to have dealers cooperate with the government and Government Liquidations, these agencies must also live up to what they agree to in their policies. In the past couple of years, many of the items buyer's have purchase, have been reclassified and buyers are now required to return the items back to Government Liquidations. We are told that our shipping expenses and our purchase prices will be refunded. This is not taking place, however. The purchase prices and fees nor the shipping expenses are being reimbursed. I personally ended up flying out to the West Coast just to talk to Government Liquidations and fight for reimbursement. I did after 7 months, finally receive partial reimbursement. I have heard about other vendors who are owed hundreds of thousands of dollars. Because of this, many vendors simply refuse to return the

> materials. I personally, have put the requested merchandise into storage, but cannot afford the shipping expenses to ship the materials back without reimbursement of my shipping or purchase expenses.

In conclusion, what we are dealing with is not an inability to enforce security measures, but a lack of policies and procedures to enforce. We don't need tighter restrictions and more limits on what can be sold, but to use common sense and understand what the actual items are that are being sold.

Mr. STUPAK. Well, thank you and thank you to all of our witnesses for your testimony, and I think it is fair to emphasize again that the industries are here, the companies are here and a representative for Mr. Fitton by himself, basically a one-man operation through ITT which a $500 million operation, did not violate any laws. Probably—and they did cooperate with GAO after we made the purchases, but we are going to try to expose some of the problems with the laws or the policies that we have and see if we can't correct them as the purpose of this hearing as we do in oversight investigation.

Let us start with questions. I will begin.

Mr. Fitton, just out of curiosity, so you bought this—the F–16 engine monitoring system computer from the government. Right? And you are cleared by the government to buy this stuff as surplus military?

Mr. FITTON. That is correct, and might I add that many of the items which I purchased over the last several years, they have recalled, such as clothing.

Mr. STUPAK. Sure.

Mr. FITTON. Such as helmet covers and things of that nature. However, sensitive items such as the F–16 engine computer, they have never asked me to return those items.

Mr. STUPAK. OK. So you buy it, and you are licensed by the government, you are checked out, you are OK. But once you sell it in the United States, as long as you sell it in the United States, there is no restriction on that. Right?

Mr. FITTON. That is correct.

Mr. STUPAK. What on God's green earth would anyone want with an F–16 engine monitoring system computer? Why would that have a resale value?

Mr. FITTON. Well, typically a lot of items which a lot of people wouldn't understand what someone would want actually go to museums, collectors, I have sold a great deal of items to movie production companies and things of that nature——

Mr. STUPAK. OK.

Mr. FITTON [continuing]. Out in Hollywood. And things such as the infra-red flags there which——

Mr. STUPAK. Right.

Mr. FITTON [continuing]. Are a restricted item——

Mr. STUPAK. Right.

Mr. FITTON [continuing]. Honestly a lot of these things I purchase from overseas countries such as China. So export restrictions are kind of curious to me simply because a lot of the things we are restricting from export we actually import into this country from the countries we are trying not to export to.

Mr. STUPAK. Right.

Mr. Kutz, let me ask you a couple questions. Your undercover investigation showed how easy it is to obtain military and dual-use items on the State Department's Munitions List and the Commerce Department's Commerce Control List. Your investigation also illustrated that our laws impose few, if any, controls on domestic sales of these items. In the post 9/11 world, I don't think it makes any sense to assume that all attacks against the United States will occur or will occur from overseas.

So in your undercover operation, your investigators bought seven items or several items that could be used to make IEDs, improvised explosive devices. Is that right?

Mr. KUTZ. Yes. Several of these have IED applications.

Mr. STUPAK. Which are those? Which items are they? I know you have some of them up here.

Mr. KUTZ. For example, the quadruple differential line receiver, you can put that on the monitor, too. It is——

Mr. STUPAK. Is your mike on?

Mr. KUTZ. Yes, it is.

Mr. STUPAK. OK.

Mr. KUTZ. It is a little chip, and I think they can——

Mr. STUPAK. OK.

Mr. KUTZ [continuing]. Put it on the monitor for you. That is one of them. The inclinometer, which I believe those are both of my left——

Mr. STUPAK. Right.

Mr. KUTZ [continuing]. There. Those are two, and I believe some of the other ones have other applications. We actually look for ones that appeared to have been going to Iran as part of prior criminal cases that were being built into IEDs and used in Iraq. That is the type of things we are talking about.

Mr. STUPAK. OK.

Mr. KUTZ. And this is low-end technology unlike some of these others. This is very low end. It is potentially available other places. Why they come to the United States looking for it I don't know exactly.

Mr. STUPAK. Well, we have many reports that these IEDs when they go off, they find U.S.-made parts in them.

Mr. KUTZ. Correct.

Mr. STUPAK. So it is a serious problem that we are facing in Iraq, Afghanistan, and elsewhere right now.

Mr. KUTZ. Yes.

Mr. STUPAK. All right. Let us take a look at some of the items you purchased. Body armor, night-vision scopes, and secure radios. Are you concerned these could be used by not just terrorists but criminals and terrorist organizations operating within the United States?

Mr. KUTZ. Yes. I do think there is—especially like the body armor seems to be more of a domestic. We didn't see any criminal cases of export of the body armor, but there is many criminal cases of—the Binghamton case recently, the shooter there was——

Mr. STUPAK. That's the one up in Pittsburgh?

Mr. KUTZ. No. Binghamton, New York.

Mr. STUPAK. OK.

Mr. KUTZ. The one where about 12 or 13 people were murdered by someone. They had body armor. We don't know what type of body armor, but body armor was used in some of the bank robberies from the 1990s you are probably familiar.

Mr. STUPAK. Oh, yes. There was legislation introduced some timeframe to restrict those sales, and we never could get anywhere with it.

Mr. KUTZ. Yes and——

Mr. STUPAK. And I know Mr. Doyle wanted to come and testify because of the recent shooting of three police officers in Pittsburgh, that individual was in the body armor that we see here today.

Mr. KUTZ. Right, and we actually have—I have a quote of actually a Craig's List ad that we had as a prior investigation, and it actually said, and I quote, "a must have for any gangster." So that is another use of the body armor that we understand.

Mr. STUPAK. OK. Ms. Lasowski, let me ask you this. You testified that GAO placed the lack of control over sensitive military targets on your high-risk list. Correct?

Ms. LASOWSKI. Yes. That is correct.

Mr. STUPAK. OK. Let me ask you about this. The Arms Export Control Act and the Export Administration Act date back several decades. Were any of these laws amended or updated at any point since 9/11?

Ms. LASOWSKI. There has not been a fundamental change in the laws. As Mr. Borman has mentioned the Export Administration Act has lapsed——

Mr. STUPAK. Right.

Ms. LASOWSKI [continuing]. And has been kept alive through executive order and——

Mr. STUPAK. Through an emergency executive order.

Ms. LASOWSKI. Exactly, and so there has not been a major overhaul of either law.

Mr. STUPAK. OK. For committee members, remember we had our hearing there in April about the chemical plant in West Virginia that blew up, and we mentioned a lot about what if a terrorist would view this as a target. Everything they wanted to do to hit that chemical plant that we had the hearing on, the night vision, body armor, IEDs, it is all there. So it goes farther than that.

We are going to try to keep the 5 minutes. We will keep going back and forth. We have votes soon, so let me go to Mr. Walden for his set of questions.

Mr. WALDEN. Thank you very much, Mr. Chairman.

Mr. Kutz, what kind of checks did some of the companies run on your GAO undercover company called Monacasey Tech Consultants? What kind of background checks, and what did the companies think those checks would show?

Mr. KUTZ. There were a variety of controls we were using. I want to start with the end-use certificate that was mentioned here. If we could put that up on the monitor, too. I actually would like to read to you. It is essentially a self-certification that you won't export, et cetera, so it says, "I confirm that the products listed above," and this was the Ka-bank amplifier, "will be so used for the end use stated above and will not be used in or for nuclear, biological, chemical weapons, or missiles capable of delivering these weapons. I further confirm that the products will not be exported."

So that was considered part of the control system to get a self-certification from us in several of these key products.

Mr. WALDEN. So if I wanted to do something bad with what I got, I would just sign this and say I promise not to use this to create a nuclear, biological, or chemical weapon. Honest.

Mr. KUTZ. That is what——

Mr. WALDEN. Signed Osama bin Laden. It would be believable and enforceable.

Mr. KUTZ. Well, we signed it in all cases, and I don't believe there are any other checks done. Some of the other things just real quickly, they had copies of our identifications, they checked to see if our credit card worked. Some of them actually checked to see that we had a Web site, and so there were some things—one actually claimed they did a background check, but I don't know how they do a background check of a person that doesn't exist. I am not sure what kind of record you would get on that. So that is the type of things we understood were happening.

Mr. WALDEN. Is there any information that companies could do or require of buyers when making a domestic purchase of dual-use items that would identify a possible export situation or deter a bad actor who wanted to buy the item in order to ship it abroad? I mean, is there—how can you stop that?

Mr. KUTZ. I think it is very difficult. I think some of the points that were made by the witnesses to my left here are valid points. Mr. Fitton, I guess, mentioned some of the things that he had said he did, and he maybe exhausted all options, and it still wasn't good enough to get us. And he appears to have a lot more training than a lot of the other people we were probably dealing with here in recognizing a kind of a situation like we were.

Mr. WALDEN. You have met with all the manufacturers and distributors who were the subject of your investigation. Correct?

Mr. KUTZ. We either met with or talked by phone after this. There were no contacts with them before the transactions.

Mr. WALDEN. While any restrictions they place on domestic sales are voluntary, do you think they were sufficient to prevent foreign nationals or terrorists from obtaining these sensitive items?

Mr. KUTZ. No, and as I think we had found based on discussions with law enforcement, the kind of front company we used and the kind of scheme we used is one that is being used by real foreign governments and terrorist organizations today. This is not a hypothetical. This is a real.

Mr. WALDEN. That is pretty disturbing.

Mr. KUTZ. Yes, it is, and again, we, again, these items we were successful with, and I think it raises questions. I mean, I think that the military and the dual-use items are different. The military, some of the discussions here about what should be done, what possible use does anybody have for whatever the U.S.—according to the U.S. military this is being used today by our soldiers. Why would anyone else need exactly what our soldiers need? That is something that has a more easy solution than the dual use.

Mr. WALDEN. Do you have your domestic buyers sign—well, I want to go to the companies.

Do you have your domestic buyers sign end-use agreements? Could you answer verbally into the microphone each of you?

Mr. ALVIS. Yes, sir. We have instituted as much out of our own experience as we learned and instituted a compliance, a rigorous compliance system. We have required our distributors, dealers, the people that we sell to, which is a very, very small part of our business, to sign end-use agreements.

Mr. WALDEN. Mr. Roush.

Mr. ROUSH. No, we don't ask for—on domestic sales of these items we don't ask for an end-use statement.

Mr. WALDEN. Really? OK. Mr. Fitton.

Mr. FITTON. Yes, I do, and contrary to something that was said earlier in the proceedings, I do require the customer to actually say what the end use is going to be. Granted, it is just what they are stating it is going to be.

Mr. WALDEN. Right.

Mr. FITTON. In this case it was for display, but that is essentially all I as a buyer from the government am required to give as well.

Mr. WALDEN. So do any of you that are selling this equipment, I realize you are following the absence of the law, it doesn't exist, do you get comfort from these end-use agreements? Do you see—do you share our concern that just because somebody signs it and says I promise I won't use this for nuclear, biological, or chemical weapons or missiles, signed Kim Jong II, what do we do here? It doesn't——

Mr. FITTON. Personally, if—this is what I am required to give to the government. If it is good enough for the government to use, shouldn't it be good enough for me to use as a reseller? And on that note a lot of the things that are considered dual-use technology and no longer authorized for the government to release, these are common, off-the-shelf items that you could be—purchase at Radio Shack, including a oscilloscope, which the government——

Mr. WALDEN. Right.

Mr. FITTON [continuing]. No longer releases, but I as a buyer sometimes get confused as to what I should be——

Mr. WALDEN. Yes.

Mr. FITTON [continuing]. Concerned with and what I shouldn't be concerned with considering some of the items up here the government doesn't seem to be very worried about where a lot of items they should be worried about they don't care.

Mr. WALDEN. I appreciate that. That is the struggle I think we are all having here because we are all under risk, at risk here.

Thank you, Mr. Chairman. My time has expired.

Mr. STUPAK. Is this agreement there is no penalty if you lie on it or anything like that? I mean, it is just something to give you some comfort. Right?

Mr. ALVIS. In our case, sir, what we would do is we would probably sever our relationship with——

Mr. STUPAK. With that buyer.

Mr. ALVIS [continuing]. That distributor or dealer.

Mr. STUPAK. But there is no criminal penalty or anything like that?

Mr. ALVIS. Not that I know of.

Mr. KUTZ. Could I comment on that real quickly? I mean——

Mr. STUPAK. Yes.

Mr. KUTZ [continuing]. The one value we have seen of the end use, it doesn't really prevent anything.

Mr. STUPAK. Right.

Mr. KUTZ. Law enforcement has used it in making criminal cases to show knowledge and intent.

Mr. STUPAK. Sure.

Mr. KUTZ. So it does have value after the fact.

Mr. STUPAK. But if I don't do it, there is no penalty involved in it?

Mr. KUTZ. No.

Mr. STUPAK. I just wanted to clear that. Go ahead.

Mr. WALDEN. Mr. Alvis, you said you would sever your relationship with the distributor, do you go back, do any of your companies go back and do random checks to see if the person who signed the agreement is actually following the agreement?

Mr. ALVIS. Our dealer agreements do require, have a proviso that allows us to come and audit and——

Mr. WALDEN. So you do audit?

Mr. ALVIS [continuing]. Check to see if they do that.

Mr. WALDEN. And you do audits then?

Mr. ALVIS. We have resource constraints as any other organization does, and we have not because—we have not done that to date.

Mr. WALDEN. Do any of you do audits back on this? I realize you are not required to but——

Mr. FITTON. Unfortunately, there is not a whole lot I as a seller can do. I am at a little bit of a different situation than Mr. Alvis in that I would actually purchase—I would be the type of customer he would sell to. Sell——

Mr. WALDEN. Right.

Mr. FITTON [continuing]. To military and law enforcement agencies——

Mr. WALDEN. Right.

Mr. FITTON [continuing]. Who are my primary buyer. But while he would essentially come to me and see who I sold it to——

Mr. WALDEN. Right.

Mr. FITTON [continuing]. I really don't have somebody I can report to such as the ATS to get information on my buyers from, and this one thing that I would like to have access to. As a firearms dealer I have got it, so why wouldn't I have it as a sensitive materials dealer?

Mr. WALDEN. Thank you, Mr. Chairman.

Mr. STUPAK. Ms. Sutton, thanks for letting us step on your time. We will give you your 5 minutes back, Ms. Sutton, for questions.

Ms. SUTTON. Thank you very much.

Mr. Kutz, I am sitting here in a bit of astonishment at what your undercover investigation was able to buy right here in the United States, and if you just look at these tables, a detonator for a nuclear bomb, an accelerometer used in a nuclear weapons program, a steering instrument for a guided missile, components for an IED, bulletproof vests, secure radios, and night-vision equipment. It is as if our own country has become a terrorist bazaar.

Mr. Kutz, I know you do this for a living, but you were surprised at your success—were you surprised at your success in obtaining these items?

Mr. KUTZ. In some cases probably, other cases, no. We have done work on eBay and Craig's List. We have bought these same types of items there. We have actually bought from the Surplus Property System from the Department of Defense before when they were selling F–14 parts, and that was one of the reasons I believe Congress passed a law——

Ms. SUTTON. Right.

Mr. KUTZ [continuing]. Prohibiting the Department of Defense from selling F–14 parts, which had only one customer, Iran. And so not really would be my answer.

Ms. SUTTON. Well, your investigation is just so important because it shows the whole picture, you know. You found that all of these items can be easily and legally purchased inside the United States, and I want to thank the companies who are represented here today for your cooperation with the committee and for your willingness to look at making changes to the law.

But you, too, are looking at this issue through your more narrow viewpoints and with respect to your products, and I think the lesson here is that we need to look at this issue holistically, and I think Ms. Lasowski, you would agree. We need to see the bigger picture. Each year billions of dollars in military and dual-use items are exported from the U.S. as has been made clear here today, and for too long we have viewed the problem through isolated stovepipes.

And Ms. Lasowski, you are also from GAO, you have analyzed this problem from the perspective of a federal agency coordination, and I think you are finding support that Mr. Kutz's undercover investigators, all that they found, you know. Every 2 years GAO issues what is called its high-risk report. It has been referenced, and in this report you list some of the biggest problems in government. You have placed the security of our sensitive military technologies on this list.

And I want to just read very quickly a portion of your testimony that explains why. You say this, "Poor interagency coordination, inefficiencies in processing licensing applications, and a lack of systematic assessments have created significant vulnerabilities in the Export Control System. Now, Ms. Lasowski, the Departments of Defense, State, Commerce, Homeland Security, Treasury, Energy, and Justice all have a role in regulating exports of defense-related technology, yet their coordination is poor. Can you tell us why?

Ms. LASOWSKI. Thank you for the opportunity to respond to that. What we have found over the years is that for various aspects of the Export Control System there has not been a good coordination for agreeing upon, for example, the jurisdiction of certain items or for enforcement actions. Some of the individual agencies have taken some actions towards making some improvements, and we certainly applaud any individual agencies' attempts to improve inefficiencies or an ineffective part of the system.

However, for something as important as this, it really is important to get all the stakeholders to look together at this particular topic, and what we are calling for is a reexamination of the system, and this would entail bringing each of those agencies together to represent their particular viewpoints and bring their knowledge and expertise to the topic. But then in addition what we have done here, too, is we have addressed this issue with the Office of Management and Budget. They, in turn, have informed us that given that there—this is a cross-cutting type of issue, the National Security Council may have an important role to play in this reexamination, and we welcome that opportunity for bringing all the players together to come up with solutions to the vulnerabilities and weaknesses that we have identified over the years.

Ms. SUTTON. OK, and you mentioned that there have been failures to conduct systematic assessments, and that that failure has caused significant vulnerabilities, and if you could just expand upon your answer a little bit, could you tell us what assessments they should be doing?

Ms. LASOWSKI. What we are calling for in terms of those assessments is to determine how effective their system is. The system has a particular mission and goals and objectives, and it would be important to identify the appropriate measures for figuring out are they meeting their mission and their objectives, and so what we would be asking for is to take a look at the current environment, to develop measures that would determine whether they are being efficient and effective in the current environment, and then periodically measure those to see if they are making improvements.

Ms. SUTTON. I thank you. My time is up.

Mr. STUPAK. Thank you, Ms. Sutton.

Mr. Gingrey, for questions, please. Five minutes.

Mr. GINGREY. Mr. Chairman, thank you.

Mr. Borman, do you have any sense about the number of legitimate transactions that these products go through for legitimate purposes as part of their normal production or the supply chain? I would just like to get a sense of how often these products may need to change hands before they reach their end use.

Mr. BORMAN. In general terms, of course, we have just received a copy of the report and heard the report today, so we will have to look at this in detail, and, again, I am talking about on the dual-use side really, the items on this table, not the items on this table. But a lot of these are components, so it is very likely that they will go through several iterations either from the manufacturer to a distributor or to a sub-vendor who then puts it into a sub-system and so on.

But one of the things we did look at in thinking about the scale of domestic commerce, just to give you two examples, last year it was estimated that the domestic market for semiconductor goods was almost $40 billion. That is just the domestic market. The domestic market for aerospace goods, about $35 billion. So, you know, when you are talking about dealing with domestic, potential domestic controls on at least the dual-use items like this, that is a significant challenge.

Now, others of these are more specialized, and maybe some of the products like the triggered spark gap are more specialized, and they really just go from the manufacturer to an original manufacture equipment in OEM, and that—there is only one transaction there. So it really varies, but these kinds of things I think, the accelerometers, certainly the QRS–11 chip, which goes into a component that then goes into civil aircraft, you are talking about several stages usually.

Mr. GINGREY. Let me do a follow up on this same question, particularly for these items that we are talking about that have the domestic commercial use.

Is there any kind of a protocol or oversight of their ultimate disposal process? Because at some point the technology is going to either malfunction or exhaust its primary purpose, and it would like-

ly need to be discarded. Should this—is this an area that we should be concerned about?

Mr. BORMAN. Well, again, I think there is a distinction to be made at least currently between those things that are exported and those that are used commercially. So, for example, the QRS–11 chip, that is probably in thousands of commercial airliners around the world; Boeings, air buses, Embraers, also Commadiers. To the extent they are operating domestically and the companies need to replace them, again, that is one set of circumstances.

If they are going to be replaced abroad, then, again, they are subject to the Export Control System, and so there are certainly requirements that if companies want to export them to replace them in China or some other country, they have to go through that process.

Mr. GINGREY. I was referring to those who were primarily for domestic use.

Let me go to—and thank you, Mr. Borman. Mr. Fitton, thank you for being here today. As the sole employee of your business, I know it certainly had to make a sacrifice to get up here, and we know that this committee appreciates your presence and your testimony.

In light of what you said, it seems to me that you took most every possible precaution that you could to evaluate your buyer, the end user. Take a moment and further expand on the current limitations that a reseller faces in validating the information and the background of a potential buyer. You touched on that just a little bit a minute ago. Could you elaborate in the remaining time that I have got?

Mr. FITTON. Correct. Say if you are dealing with a firearms transaction, an individual has to fill out what is essentially an end use certificate stating that there is nothing preventing them from purchasing the weapon or any of this type of business. They have got their Social Security number, their names, their addresses, everything is listed on that application. That application is then submitted to the ATF for approval. This may be instantaneous approval, and in many cases take a week or 2 weeks for that approval process to take place.

This is no reason that we can't go through a similar process to at least validate the person purchasing that item. Now, what happens beyond that point, let us face it. If somebody wants to do some nefarious activities to the U.S., they can do it. There is no way to prevent this in its entirety. All we can do is try and do as many measures as possible, and one of the things that we have to look at is the fact that there are terrorists that are trying to destroy America, there are individuals throughout the world who want to see our downfall, but our current political correctness and the fact that we do have so many privacy rights protecting American citizens, these privacy rights are also protecting the terrorists, and we are not able to actually hunt down the real cause of what is causing damage to the countries. It is not the items. It is the end user, simply because I could do more damage with a truck full of fertilizer and gasoline than I can with any of the items that have been brought up on display today.

Mr. GINGREY. Thank you, Mr. Fitton, and I yield back, Mr. Chairman.

Mr. STUPAK. Thanks, Mr. Gingrey.

Mr. Braley for questions, please.

Mr. BRALEY. Thank you, Mr. Chairman. Mr. Alvis, I appreciated your comments about some of the changes that have been made at ITT, but you may want to count me as someone who is still skeptical about the progress that is being made, and I want to talk to you about that.

In 2007, your company was convicted of one of the biggest criminal violations in the history of the Arms Export Control Act for illegally exporting to China and other countries technology relating to your highly-sought-after night-vision goggles, and the company was fined $100 million. And I want to show you what Daniel Wilkins at the Defense Criminal Investigative Services said about your company. He said this, "The illegal export of U.S. military technology and equipment threatens our national security in the most direct way. Americans' security and its critical military technology are simply not up for sale."

And Julie Myers, who was the assistant secretary for U.S. Immigration and Customs Enforcement at the Department of Homeland Security said that your company placed profits ahead of the security of our Nation.

So my question for you is are you here today to vouch on behalf of ITT that those concerns are no longer valid about your company?

Mr. ALVIS. Yes, we are. The people that were involved are no longer with the company. I talked earlier in my opening statement about the structure we put in place. I was not there. I've only been there 2½ years. I was redeployed there along with—our entire senior staff has come on board within the last 3 years to include our president.

Mr. BRALEY. OK. Well——

Mr. ALVIS. We are totally—yes, sir. That——

Mr. BRALEY. Let us talk about that. Here is another quote from Kenneth Wanstein, who is the assistant attorney general at the Department of Justice, and he said, "ITT's exportation of this sensitive technology to China and other nations jeopardized our national security and the safety of our military men and women on the battlefield," which is an extremely strong statement coming from the Department of Justice.

And what I don't understand and what the committee doesn't understand is your company is still doing business with the Federal Government. Correct?

Mr. ALVIS. That is correct.

Mr. BRALEY. And the Justice Department allowed your company to defer $50 million of that $100 million criminal fine by allowing you to invest it towards a new, more-advanced line of night-vision goggles. Isn't that true?

Mr. ALVIS. That is true.

Mr. BRALEY. Now, normally when a company is convicted of illegal activities of this magnitude, they are automatically debarred from future government contracts. Why hasn't ITT been debarred, according to your understanding?

Mr. ALVIS. As I mentioned in my opening statement and my written statement, we are the world leader, and we have made drastic changes. One of the things that I think the government believes, and this is my opinion, is that the heart of the night-vision technology was not compromised. The goggle is nothing but a wrapper for the tube. The tube is the essence of the goggle. The tube cannot be reverse engineered. The tube is—and the government is convinced of this. I have talked to the former customer general officer level, that the security of the United States was not compromised via any of the activity.

Mr. BRALEY. Well, that would seem to de-lie $100 million fine, which apparently was levied in connection with the activity. Wouldn't you agree with that? That if there is no compromise of the national security, why in the world would $100 million fine be imposed?

Anyway, let me move on. This isn't the only time that ITT has been engaged in illegal export activities. The committee requested from the Department of Commerce copies of documents relating to other ITT export violations, and one of the documents shows that in 2007, which would have been within the timeframe you are talking about after this changeover in management at the company, one of your subsidiaries, Engineered Values Group, was fined for illegally shipping valves used in chemical and biological weapons to China, Israel, Saudi Arabia, and Taiwan. Isn't that right?

Mr. ALVIS. As I mentioned earlier, I am in the night-vision business area. I have no knowledge of that.

Mr. BRALEY. But that certainly would have been within the period of time that you have indicated the company has had a change in management if it happened in 2007.

Mr. ALVIS. We can respond to that question and get back to you for the record. I really don't feel comfortable, particularly under oath, responding to something I have no knowledge about.

Mr. BRALEY. All right. Then, Mr. Chairman, I would specifically request that we get an official response from the company in regard to that question.

Mr. Kutz, let me close with you. After ITT's conviction and $100 million fine, the company officials issued a statement saying they had conducted a comprehensive review of their policies and procedures and were initiating new monitoring to prevent illegal exports. But in November, 2008, which is even later than this 2007, incident, you were able to purchase their night-vision technology from one of its distributors using fake company and fake individuals' identification. Isn't that true?

Mr. KUTZ. Yes, and in fact, we became a distributor.

Mr. BRALEY. So, Mr. Chairman, that illustrates why I continue to have serious concerns about ITT's actions. The company's history of illegal exports is troubling and raises serious questions about whether it continues to put profits over the security of our Nation.

And in closing, Mr. Chairman, I would just like to point out that while this hearing has been going on in response to the memo we received from the committee, I drafted a very simply certification that I think could address many of the issues that have been raised here at the hearing today. It would require the name, address, phone number, e-mail, business address, employer identification

number of anyone purchasing these items, and it simply states in a very short form, "I understand that the item I am purchasing is, A, a defense items under the Arms Export Control Act, or B, a dual-use item under the Export Administration Act. I also understand that this item is subject to export control laws that may prevent or restrict the sale or delivery of this item to anyone outside the United States. I am aware that I may face criminal prosecution and or civil fines and penalties if I attempt to sell or distribute this item in violation of these export control laws, and I certify that neither I nor anyone on my behalf will attempt to export this item at any time."

Now, there is a paper trail that would certainly add some teeth to prosecution and enforcement of anyone attempting to violate our laws.

And with that I yield back the balance of my time.

Mr. STUPAK. Thank you, Mr. Braley.

Mr. Burgess for questions. Five minutes, please.

Mr. BURGESS. Thank you.

Mr. Alvis, we heard I think it was Ms. Lasowski testify that the exporter determines the level of government review. Is that—do you generally agree with that?

Mr. ALVIS. That the company——

Mr. BURGESS. Yes. That the exporter, the person who is doing the export of—exporting the item in question is—because of the ambiguity of our laws and the problems with jurisdiction, that many, much of that is left up to your discretion. Is that a fair statement?

Mr. ALVIS. On the exports it is pretty specific. On our international business we sell to the U.S. Government which sells to other governments as a government-to-government sale through the Foreign Military Sales Program, but we also do direct sales to other militaries. ITT is in the business of selling to militaries overseas. We can sell to them directly, but the ITAR that I mentioned earlier does have provisos. Every time you ship an item, every time you get an order from an international customer, you apply to the State Department to receive an export license. Each export license is handled on a case-by-case basis and can have specific provisos in it that regulate the technology. So we just respond to whatever our government determines.

Mr. BURGESS. And do you think that is an adequate safeguard the way that is set up, or would you structure something different having come through the experience that you have endured?

Mr. ALVIS. From my personal experience having used these goggles as a military officer and also—and having been down in the night-vision business for the past 2½ years, my personal opinion is that the ITAR is rigorous enough with its figure of merit calculations. A lot of people don't know that the stuff we export, even to our closest allies, is not the same night vision that the U.S. military gets. The goggle may look the same, but the tube inside—we made 200 different types of tubes of varying degrees, all the way down to the ones which I would not consider to be cutting edge that we sell commercially, to the best tube that the U.S. military gets.

So my personal opinion is that the ITAR is rigorous enough to control the export of night vision.

Mr. BURGESS. OK. Let me ask a question. I guess, Ms. Lasowski, I need to direct this to you. You talked about the turf battles that go on between Commerce and State. I guess, Mr. Chairman, I don't really understand why we don't have the State Department here today. Perhaps that would be helpful, but is this a frequent occurrence that these turf battles occur between Commerce and State?

Ms. LASOWSKI. We have noted various instances where there have been jurisdictional disputes that have occurred. Sometimes it has occurred due to some confusion about where space technology, for example, is controlled. But the instances that I was referring to had to do with actually an exporter who became aware that his competitor of the very same item was going through the Department of Commerce and utilizing that system to export his item, while this other company was going through the State Department.

Mr. BURGESS. So they were at a competitive disadvantage.

Ms. LASOWSKI. They were at a competitive disadvantage, and therefore——

Mr. BURGESS. Do you get——

Ms. LASOWSKI [continuing]. In that kind of situation you have an unlevel playing field——

Mr. BURGESS. Sure.

Ms. LASOWSKI [continuing]. And that is why I referred to the exporter as being really the first step in terms of deciding which process to use.

Mr. BURGESS. Because they can venue shop or, I am sorry, agency shop as to the most expeditious way to get their product out.

Ms. LASOWSKI. It is a complex system, and it is up to them to be—to understand the export control laws and regulations.

Mr. BURGESS. Why is it like that? Why is there a dual jurisdiction?

Ms. LASOWSKI. That has been——

Mr. BURGESS. I am just a simple country doctor, and so tell me, why did we set it up like that? When did it happen, why did it happen, was there something we were trying to accomplish by setting up this dual jurisdiction?

Ms. LASOWSKI. The system is bifurcated because they are to accomplish different activities. The State Department is to control the most sensitive defense items, while the Commerce Department is to control those items that are commercial and military applications.

Mr. BURGESS. But has it always been that way?

Ms. LASOWSKI. The system has been established, yes, as that long ago.

Mr. BORMAN. Sir, if I could just add a little bit to that.

Mr. BURGESS. Yes.

Mr. BORMAN. The Export Administration Act originally was passed in 1949, but it is a Cold War statute as I mentioned. The Arms Export Control Act actually predates World War II, and as Ms. Lasowski said, they originally had different purposes. One of the challenges now is, of course, you have so much commercial, off-the-shelf technology going into military systems and conversely, you have some military systems moving back into the commercial area, and that is a big difference over the last 20 years.

Mr. BURGESS. Now, when I was just a regular person and not in Congress, I mean, I seem to recall a lot of controversy back in the '90s about selling satellite technology to China. Did we not get into some of this same difficulty between Commerce and State with selling the satellite technology to BRC back in the '90s?

Ms. LASOWSKI. That is correct. The late '90s there were export violations that occurred and then the Congress passed legislation to change the jurisdiction of satellites and related components from the Commerce Department to the State Department.

Mr. BURGESS. Well, was that fix then just inadequate, that it should have been a broader fix that has led us now to these additional problems that we are discussing today?

Ms. LASOWSKI. I think the best thing—response that I would have for that is that we are calling for a reexamination of the system and the whole safety net of programs, and as part of that one of the first key steps is determining what is it we want to control and how do we want to control it, particularly given the challenges of the 21st century.

So it would be a good set of questions for the agencies that are responsible to come together and discuss to see if they are—if the current structure best supports the current challenges.

Mr. BURGESS. That is an excellent piece of advice.

Mr. Chairman, I am just concerned that 10 years ago Congress took it upon itself to fix this problem, and here we are 10 years later, and the problem is not fixed, and people are put at risk, and fines are being levied. It seems like an inconsistent way for us to be doing business. So I hope we take this problem seriously, and I just thank the witnesses for being here today. I think it is a terribly important issue that we need to get resolved.

I yield back.

Mr. STUPAK. That is why we are having the hearings, and we hope to have some resolutions.

Mr. Markey, for questions, and Mr. Welch, I want to try to get you in, too, before votes.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. Borman, as you know, I have been a long-time critic of your bureau's validated end-user program which allows certain foreign companies to import certain controlled U.S. goods without individual export licenses. Of the five Chinese companies originally certified as validated end users, two were found to be closely affiliated with China's military industrial complex, and two companies that had been under U.S. Government sanctions for proliferating WMD-related technologies.

Apparently, these bad background checks by your bureau are continuing. On April 24 you signed an order which added a new Chinese company, Avesa Technology, to the program, that is this validated end-user program, which basically says we trust you. We are not going to put you through the full process.

The order named five import destinations that Avesa was authorized to receive certain sensitive U.S. goods without export licenses. Here we are talking about a pressure transducer, which is used in uranium enrichment.

Are you aware that one of the import locations that you authorized to receive a pressure transducer is also listed as the address

of a company that the United States sanctioned by the State Department in December of 2006?

Mr. BORMAN. Mr. Markey, the validated end users go through an extensive review with many agencies including the intelligence community and——

Mr. MARKEY. Are you aware that one of them was sanctioned in December of 2006?

Mr. BORMAN. I don't believe that is correct, sir, that any of those validated end users, the ones that we approved, were sanctioned by the U.S. Government, because if they were, they wouldn't have been approved.

Mr. MARKEY. OK. Then I have here pages and pages of documents that show this Chinese company called CEIEC International Electronics, which has been sanctioned by the State Department, is headquartered at the exact address that you have now authorized to receive certain sensitive, dual-use, high-technology U.S. products. The location that you have authorized to import sensitive U.S. goods, including pressure transducers, which are extremely important to uranium enrichment, is Building A–23, Buxing Road, Beijing. And these documents show the exact same address is the headquarters of a company that has been sanctioned by our government for WMD-related proliferation, Building A–23, Buxing Road, Beijing.

These documents were provided to me by the Wisconsin Project on Nuclear Arms Control, which was the organization that originally blew the whistle on your VEU Program.

How is it that this small NGO can consistently do a better background check on these Chinese companies than you can do?

Mr. BORMAN. Well, I have to say respectfully I disagree that they can do a better job. We would be happy to take a look at what information they provided you, they have not provided to us, but what I can tell you is all of those validated agencies go through a thorough interagency review, including the intelligence community. So right now today I can't discuss this with you. We would be happy to look at it, but I can tell you that, again, it goes through a thorough review, and as you recall from the response our bureau gave to you earlier on the original five, there is a significant distinction between the specific entities that are approved and other entities that the Wisconsin Project is——

Mr. MARKEY. Well, you have just certified a sixth Chinese company to ignore our Export Control System, and that is essentially what this program does, ignores the Export Control System, sets up a special fast lane that doesn't have the same level of scrutiny, and it is the third one where you did not know it was associated with a company that had been sanctioned by the United States Government.

Mr. BORMAN. Well——

Mr. MARKEY. And I think that when three out of the six are, in fact, not properly scrutinized, then the program is essentially unacceptable. It is not something that should be in place, and we will share these documents with you, but it just seems to me that it shouldn't be an NGO that identifies that this new transfer is going to the exact same address as a company which was sanctioned just

2 years ago for violations of the very same type that we are talking about here today.

Mr. BORMAN. Well, again, all I can tell you is there is a thorough interagency review, including the intelligence community. We would be happy to look at that information, but I would be very surprised if this is information that really correlates as the Wisconsin Project apparently is alleging.

The other point I would like to make with the validated end-user program is very extensive review. All of these companies have extensive individual licensing history. Many of them have been visited by U.S. Government officials in an official capacity, and there is a check once things are shipped there on the back end. So the requirement is that it eliminates individual rights and requirements. They don't get a free ride.

Mr. MARKEY. Well, I just think that this whole concept of validated end user that allows for a circumvention of a full inspection is a very questionable process. It would be like being at the airport and them being able to say, well, you don't have to go around, you don't have to go through the full screening, you don't have to go through the full screening, but all the rest of you do. Well, if you are going to have a program like that, then you cannot have mistakes. You cannot have—there ought to be a trusting relationship which is developed where the same address 2 years later is receiving materials that could be used in uranium enrichment in a country about which we still have questions in terms of their nuclear non-proliferation record.

So I thank you, Mr. Chairman, very much. I just have very serious questions about this validated end-user program. I think it ultimately turns into a validated end-abuser program if, in fact, you can have violations like this, and I will share the material with you, and I look forward to getting a response.

Thanks, Mr. Chairman.

Mr. STUPAK. Yes.

Mr. BURGESS. Mr. Chairman, can I ask unanimous consent that Mr. Markey's documents be shared with members of the minority as well as the witnesses?

Mr. MARKEY. It will be done so. Yes.

Mr. STUPAK. For the record, shared with both.

Mr. Welch, for questions, please. We got votes on the floor, but let us get your 5 minutes in.

Mr. WELCH. I will try to be quick.

Mr. STUPAK. No. Take your time.

Mr. WELCH. I want to ask Mr. Kutz a few questions if I could, and it is about the nuclear weapons issues.

Two weeks ago if you note North Korea detonated a nuclear weapon during an underground test and is threatening to test fire an intercontinental ballistic missile. And what concerns me is this. Last year the Strategic Studies Institute, a component of the Army War College, issued a report about the North Korean ballistic missile program, and I don't know if you want to make this part of the record, but that report is here.

And it concluded, and this is what is relevant to us, that North Korea almost certainly depends upon outside sources for advanced electronic components and other sophisticated hardware for missile

guidance systems, and incidentally, North Korea then sells what it makes, including possibly to Iran. And the report warned that as early as 1999, North Korea was trying to procure gyros and accelerometers and other components for its ballistic inertial guidance.

And what I want to ask you is about those two items, the accelerometers and the GyroChips, those are two of the categories of items that you were able to purchase using the fake company and a fake buyer. That is right. Correct?

Mr. KUTZ. Yes.

Mr. WELCH. And I don't know if you want to put the photos of those two items—I guess you have done that.

Mr. KUTZ. I have got these over here, too.

Mr. WELCH. All right. How easy was it for you to purchase those?

Mr. KUTZ. The accelerometer there was an end-user certificate, and it was done by credit card, fictitious name, bogus company, and mailbox. So that was——

Mr. WELCH. Easy.

Mr. KUTZ [continuing]. Relatively simple I would say, and then the GyroChip, the same thing, and we got a quote for additional ones of those. So I would say that they were similar in how difficult they were to obtain.

Mr. WELCH. And is it correct that those items can be sold within the U.S. without any license?

Mr. KUTZ. Legally, yes.

Mr. WELCH. OK, and let me ask you, after you bought these items, you were then able to send them to Federal Express to a country in southeast Asia?

Mr. KUTZ. Correct.

Mr. WELCH. And I won't ask you what country it is. I know that is sensitive information, but can you tell us why you chose that specific country?

Mr. KUTZ. Because it is a known transshipment point to terrorist organizations.

Mr. WELCH. All right. So we send it there or someone sends it there, and that is a location from which it goes to people who are trying to do Americans warm.

Mr. KUTZ. Correct.

Mr. WELCH. These items are very small and lightweight. Just out of curiosity, how much did it cost to mail these halfway around the globe?

Mr. KUTZ. Fifty dollars and what we labeled them as was documents. That was the word we used on them.

Mr. WELCH. To me your undercover investigation, thank you for doing that, even though it is quite alarming, it shows that our current system does not adequately prevent the export of items that are actually used in nuclear weapons programs. Do you agree with that conclusion?

Mr. KUTZ. Yes. I mean, that is why we chose these items. We took the exact same part number out of indictments and criminal cases, and that—these two items you just mentioned are the exact same part that was cited in cases going to China, Iran, terrorist organizations, et cetera. So that was why we chose them so this was real examples of what is going on.

Mr. WELCH. Well, I really thank you. It is incredibly alarming. Mr. Chairman, it is troubling because North Korea manufactures nuclear things and then exports their technology. So I do hope and I appreciate your efforts to have a thorough review of export controls.

And I yield back my—the balance of my time.

Mr. STUPAK. Thanks, Mr. Welch. Mr. Doyle still plans on coming. I am sure there will be questions after.

We got votes here. Why don't we just recess until—about 25 minutes here. How about 12:20, give you a chance to stretch your legs. We will come right back, and I am sure we can finish up in probably within an hour after that. So I ask you all be back about 12:20.

Thank you. We are in recess.

[Recess.]

Mr. STUPAK. The hearing will come back to order. Thanks for your patience. I know Mr. Doyle has come in and I think one or two other members.

I have a couple questions. Mr. Kutz, let me ask you this if I—because one that sort of caught my eye was GAO's purchase of the infrared American flag patches. I think you have one up here. Can you pull in those on screen, what they look what?

These infrared flags can appear as a United States flag or just a black material when you look at it. Right? A black——

Mr. KUTZ. Right. They can appear as black or if you use the infrared and you turn on the——

Mr. STUPAK. Right.

Mr. KUTZ [continuing]. Specialized item that is made——

Mr. STUPAK. So show that. So it is black up there and then when you look with the infrared it comes out the American flag.

Mr. KUTZ. It looks like a U.S. flag with the goggles. Yes.

Mr. STUPAK. That is with the night-vision technology. And these flag patches are currently worn by our troops during combat to help identify friendly forces at night. What is the danger to our troops if these flags are available to our adversaries?

Mr. KUTZ. Well, certainly on the battlefield and I guess there are public statements made by Defense Criminal Investigative Service and the Department of Defense that the enemy does have these in Iraq and Afghanistan, so there is a concern that these are the kinds of things that could—they are supposed to be able to identify friendly versus foe, and if the foe has them, then they are going to look like a friend, and that is the risk.

Mr. STUPAK. OK. Now, you purchased these flags. Did you buy them in person or over the internet?

Mr. KUTZ. Internet.

Mr. STUPAK. How many did you purchase?

Mr. KUTZ. We purchased several, but we got a quote for 400. They were going to ship us 400 if we wanted them.

Mr. STUPAK. OK. So you got 400 and then you put an offer for—I mean, you had four——

Mr. KUTZ. Like four, eight, but we——

Mr. STUPAK. OK, and then you offered to buy 400, and that——

Mr. KUTZ. Yes.

Mr. STUPAK [continuing]. Was approved?

Mr. KUTZ. Yes. They would have shipped us 400.

Mr. STUPAK. It seems that there aren't really any legitimate reasons for anyone other than our service men and women to have these flags, is there?

Mr. KUTZ. No, although I think this is probably considered lower-end technology now. It is apparently exactly what is being used by our soldiers according to the Department of Defense officials we spoke to.

Mr. STUPAK. Were you required to show that you were a member of the Armed Forces in order to buy them?

Mr. KUTZ. The agreement that this distributor had with the manufacturer was that they required a military ID, but this distributor did not request a military ID from us, and so we were not—we did do a counterfeit military ID in another case, but in this one they were supposed to, and they didn't. According to the manufacturer, this will no longer be a distributor of theirs.

Mr. STUPAK. Like I said, this one sort of caught my eye because no one really needs this except maybe your military people. So I asked our staff to do some research on this, and this—here is what they tell me.

First, anyone can buy these legally in the United States. Correct?

Mr. KUTZ. Correct.

Mr. STUPAK. And you cannot export these items to certain countries like North Korea, China, or Afghanistan. Correct?

Mr. KUTZ. These are on the Commerce Control List, I believe.

Mr. STUPAK. OK, but you can export these flags to countries like Saudi Arabia, Yemen, and Cambodia. Is that correct?

Mr. KUTZ. I don't know the difference in who you can ship it to——

Mr. STUPAK. OK.

Mr. KUTZ [continuing]. And who you can't.

Mr. STUPAK. Well, let me ask you this then. Does it make any sense that you can—you can't export to North Korea, China, or Afghanistan, but you can to Saudi Arabia, Yemen, Cambodia. They are readily available here in the United States even though there really is no use for it, I guess, as far as military and for identification. If we believe our adversaries shouldn't have these, I think it is a pretty bizarre way to implement that goal, and I really think it highlights why we think we should reexamine the entire system for controlling items that only have military uses.

Mr. KUTZ. Yes. I concur with that. I think that many in the military and especially the soldiers concur. I don't think that they are excited about the items that they use on the battlefield today being so readily available. That is something that is a concern.

Mr. STUPAK. Mr. Fitton, would your customer base be interested in these?

Mr. FITTON. Actually, the largest percentage of my customer base is military and law enforcement, and in the past I have had difficulty getting these from U.S. suppliers. I have purchased them directly from China. So——

Mr. STUPAK. So they export back you are saying.

Mr. FITTON [continuing]. No matter what exports you restrict here in the U.S., it doesn't make a difference if a Chinese person

can buy it directly from their own country. So our export regulations won't affect this market whatsoever.

Mr. STUPAK. Buy from their own country. Do you know if they are manufactured in China?

Mr. FITTON. Yes. They are manufactured in China.

Mr. STUPAK. So you just export them back here, and you can——

Mr. FITTON. Right. This is not high-tech technology that only the U.S. has access to. Countries around the world produce IFF flags and patches for——

Mr. STUPAK. But then in order to view it or to see it, you have got to have night vision, don't you?

Mr. FITTON. Correct.

Mr. STUPAK. And I take it not very high-tech night-vision goggles, just probably any night vision.

Mr. FITTON. Correct. Gen 1, Gen 2, or both will reflect it.

Mr. BORMAN. Mr. Stupak, if I could just add an observation.

Mr. STUPAK. Sure.

Mr. BORMAN. Based on what I have just seen and heard, I think it would be more likely that those items would be on the U.S. Munitions List and not on the Commerce List. Because the definition for a military item is specifically designed for military application, and off the top of my head it would seem to me that is exactly what those things are. Just a little correct there or observation.

Mr. STUPAK. But either way they are on a list, they are restricted but readily available, or we can bring them in from China if we wanted to. So there is plenty of opportunities for our adversaries or terrorist groups or whatever, domestic or foreign, to get them, to use them to harm Americans.

Mr. Doyle has arrived. I know the Penguins aren't going to show up for the game tonight, but I am glad to see you did, so if you would like to ask some questions, now would be a good time.

Mr. DOYLE. Later, my friend, have your fun now because tonight you are going to be crying in your beer.

Mr. STUPAK. Are those Penguin colors you are wearing?

Mr. DOYLE. Black and gold. Yes.

Thank you, Mr. Chairman. Mr. Chairman, on April 4 in my district three Pittsburgh police officers were killed and two others were injured by a heavily-armed man who fired on them as they responded to a domestic disturbance call. The three officers who were murdered in the line of duty left five children without their fathers. The standoff between the armed man and the police units lasted for hours that morning. SWAT officers were pinned down by a hail of bullets, and the wounded policemen lay where they fell. It was complete chaos.

But the gunman, armed with an AK–47 and a number of handguns, was protected. Although the gunman had been shot in the chest and the leg, he wore a bulletproof vest to shield them. The gunman was able to continue to fire on the police as a result of this protection he was wearing.

Now, Mr. Kutz, you were able to purchase a bulletproof vest over the internet, and you could have acquired the protective inserts from the same company, enabling it to withstand even heavy ammunition.

Could you tell me how did you purchase these bulletproof vests?

Mr. KUTZ. We actually in this case represented that we were part of an active reserve unit and provided counterfeit military documentation, and we were shipped this item along with the commitment to ship 20 more.

Mr. DOYLE. Had—did they do any background check on you?

Mr. KUTZ. I don't know. Well, the military ID seemed to be what they were looking for.

Mr. DOYLE. What threats do you think these bulletproof vests pose to our emergency first responders and military?

Mr. KUTZ. I think this really is a domestic threat. Again, I mentioned earlier when you weren't here that there—we didn't seen any export cases for these items. We see these more as a domestic threat, something that, you know, the military's best body armor here, the ESAPIs are the newer plates that have additional protection from the regular SAPIs, and this is what the Marine Corps uses today. It is hard to understand why anybody but military and potentially law enforcement would have a use for those.

Mr. DOYLE. Thank you. Three officers from my district were killed and two were wounded by a man who was able to continue this onslaught because he had the same product you were able to buy off the internet. I see no reason, Mr. Chairman, why criminals should be able to buy bulletproof vests for use on our streets, just as terrorists overseas should not be able to acquire them for use on the battlefield.

Mr. Chairman, for the sake of brave Americans who make our country and community safe, including the three brave officers from Pittsburgh who died in the line of duty, we have to do more to keep this equipment out of the hands of criminals and terrorists.

And I yield back.

Mr. STUPAK. Thank you, thank you, Mr. Doyle, and Mr. Kutz mentioned earlier the gunman up in Brighton where he killed about 12, 13 people, same thing, body armor. I mentioned James Gelf legislation, the San Francisco police officers on a bank robbery where there was almost like a robo-cop, just head to toe, and they got them through the mail. And we tried to restrict that with the James Gelf legislation I had a few years ago. We could never really put any severe or—curtail it, and I agree with you, and that is one of the purposes of looking at it, and I know a number of members have mentioned both—not just terrorists but also criminal activities with being able to purchase these items.

So we will continue working on it, and thanks for your input.

Mr. FITTON. Mr. Chairman.

Mr. STUPAK. Yes.

Mr. FITTON. Might I? As a dealer for these items, I do have serious reservations when you start restricting strictly to law enforcement and military. The reason for this, one of the primary consumers I have interested in body armor right now is not civilian, it is not military and law enforcement because they are typically supplied with these items. It is first responders such as EMT and firemen.

Typically in active-shooter situations and things of this nature they are some of the first people that are on site. Gunmen will typically fire at anyone in uniform or of a government capacity. Once you restrict them to military and law enforcement, all the sudden

these individuals are no longer authorized to use, as well as contractors serving overseas in security details, as well as VIP protection details here in the United States.

So we have to really address a fine line when we start doing restrictions to make sure individuals who do have a need for these items can still obtain these items, and that is something we tend to forget about when we think just tactical situations involving military and law enforcement.

Mr. STUPAK. No. I—we are cognizant of that fact, and but there is no reason why this stuff should be purchased without some kind of identification, verification of who they are. Just going on the internet I think what we have seen is if you have a credit card that is valid, they will accept the purchase. We don't care who you are, and this committee has shown time and time again everything from cat, Viagra for our cat, as long as have—that cat has a credit card, he got his Viagra. And that is the problem we see. It is not just in this area. We see it in drugs, we see it in pornography, we see it in gaming, we see it in e-commerce, and there is some legislation we are working on to really put some kind of restrictions on this credit card or verify the individual using that credit card before he can even use it.

So there is other areas we are looking at, so while we have this hearing, the purpose of this hearing was military and dual-use technology, we still go back—it filters in many of the areas of jurisdiction this committee has. And so we are trying to look at the whole thing.

But you are right. You are right.

Mr. Roush.

Mr. ROUSH. Yes. If it is possible, I would like to just clarify one point. I think a lot of excellent points have been raised by the committee today, but there is one factual point I did want to clarify. The triggered spark gaps were mentioned in the GAO's report. We didn't get the chance to see the report ahead of time. There is a few things we want to clarify.

Triggered spark gaps are not used as detonators for nuclear weapons. In fact, Perkin Elmer has an entirely separate product line that is completely ITAR controlled and not available for commercial sale that is used in conjunction with nuclear weapons. Triggered spark gaps are primarily used in medical equipment, lithotripters, which are treatment devices for kidney stones, and there is a second use of the product on conventional munitions which accounts for the minority of its sales.

I just wanted to make that clarification.

Mr. STUPAK. Well——

Mr. KUTZ. Sir, could I just comment briefly?

Mr. STUPAK. Sure, and I want to get into that a little bit because there's the Central Contractor Registration Database which sort of looks like it is like government-approved site, and we are buying the stuff.

Go ahead.

Mr. KUTZ. I don't know if the manufacturer knows why these purchased, but the source of information we used was the Department of Commerce and Justice saying that these items could be used, and I will just for the record, if you want me to submit it for

the record, I would, too, but according to the indictment the triggered spark gap and the exact model number we bought could be used as a detonating device for nuclear weapons as well as other applications. And the testimony of Christopher Podea in 2007, asserted the same thing for the Department of Commerce.

So, again, whether it was designed for that and could be used, again, I am not an expert at that, and I would certainly defer to the manufacturer to what it was designed for.

Mr. STUPAK. Well, whether it was the triggered spark gap or a couple of these other items we purchased which are sort of technical, a lot of them fall on this Federal Central Contractor Registration Database, which is an approved government supplier via the General Services Administration Schedule. It seems to me like if you are on this Central Contractor Registration that somehow you have—it is government approval, but yet you are able to purchase it like there is no—it is like the government is approving what you are doing but yet you can purchase anything you want off this CCR Registration.

Shouldn't there be some safeguards in there that if a company is on a CCR, this database that is government approved, that there is some restrictions on how they do the sales or something? Or even licensing?

Mr. KUTZ. The Central Contract Registry is something—actually a lot of our undercover companies are in the Central Contract Registry. I mean, no one validates anything in there. There is approved GSA vendors that go through a little bit more stringent process. So there is a distinction between the CCR and an approved government vendor, I believe, but to do business with the government you have to be registered in the Central Contract Registry.

Mr. STUPAK. So if you are registered, doesn't it give it some form of legitimacy to the outsider?

Mr. KUTZ. It does, and we use that all the time. We say we are registered in the Central Contract Registry, and it is similar to your IRB hearing several months ago where we were registered with HHS and assured.

Mr. STUPAK. Right.

Mr. KUTZ. It did mean something to people who look at it.

Mr. STUPAK. Well, let me ask you a little bit about this, a little bit about know your customer, Mr. Borman, and I think it is tab number five. Do we have a book up here? On the far end. Mr. Fitton, could you pass that book down?

Look at tab number five because it is some helpful hints that you get from Commerce and all that on—to know your customer, and we just have parts of your form there. It is about a 40-page form. We have certain parts of it in there, and I think it was page 38. I want to highlight a few portions of this guide.

First it says, "Absent red flags, there is no affirmative duty upon exporters to inquire, verify, or otherwise go behind the customer's representations." It also says, "You can rely upon representations from your customers and repeat them in the documents you file unless red flags oblige you to take verification steps."

So, Mr. Borman, do you think this guidance is adequate given the GAO was able to, you know, basically subvert that, know your customer?

Mr. BORMAN. Well, I think it goes back, Mr. Chairman, to what I mentioned earlier. I think the first issue would be for us does existing legal authority, that is the statutory authority we have, give us the authority to do anything differently? In this case extend regulations in a significant way to domestic transfers. And that is something that we would have to look at very carefully to see whether the existing authority goes that far.

Mr. STUPAK. OK. Well, GAO is able to convince these companies to sell sensitive military technologies every time it tried in all 12 cases. The Commerce Department guidance also lists—also includes a list of red flags for companies that—for companies to look for, and I think it is page 40 there, maybe the last one there.

For examples, custom—companies should be on the lookout if, and "the customer is willing to pay cash," or "the customer is reluctant to offer information about the end use of the item." By posting this guidance on the internet, aren't you really informing terrorists and criminals how to beat the system?

Mr. BORMAN. Well, I think the issue is, though, we do want legitimate companies to have some specific guidance from the government, and it is very difficult, I think, for us to identify the thousands, if not hundreds of thousands of U.S. companies that do business and sort of repeat individually to them, and it seems to me the Perkin Elmer example we talked about earlier exactly shows the benefit of these kind of—because it is that kind of information that they have incorporated with their product and to their corporate compliance program that said there are some red flags on that particular transaction, they contacted our field office in Boston, and that is exactly what we want to have happen.

So, I mean, I suppose you could take the position that, sure, bad guys can read this and figure out, oh, I know how to get around this, but——

Mr. STUPAK. Right.

Mr. BORMAN [continuing]. You know, I think it is more important to have all—the vast majority of companies in the United States that want to do legitimate business to have this information available to them so that they do come to us, and that is a lot of our cases as Mr. Madigan can tell you——

Mr. STUPAK. Sure, but——

Mr. BORMAN [continuing]. Come from tips from U.S. companies.

Mr. STUPAK [continuing]. It just shows you how much the internet has changed. I mean, if you take the way we do business, all—most of these purchases were on the internet or over the internet. Right, Mr. Kutz?

Mr. KUTZ. Yes. For all the purchases we made——

Mr. STUPAK. Yes.

Mr. KUTZ [continuing]. We never spoke on the phone or met face to face with anyone. It was all fax and e-mail transactions.

Mr. STUPAK. So it almost made the red flag almost—you can get around it so easy.

Let me ask this. Mr. Roush, if I will, you represent Perkin Elmer, the company that sold the trigger spark plug gap to GAO, a fake company. Your company adopted the Department of Commerce guides right there on tab five and created your own customer screening procedure.

Mr. ROUSH. Yes.
Mr. STUPAK. Right.
Mr. ROUSH. That is correct.
Mr. STUPAK. OK. Do you agree that both your guidance and the Commerce Department guidance was inadequate? Would you agree with that?
Mr. ROUSH. Well, I would say it doesn't protect against the kinds of examples that you are talking about; if somebody were to try to buy a product under a legal transaction and then subsequently illegally, you know, use it for a unintended use or export it——
Mr. STUPAK. Sure, but——
Mr. ROUSH [continuing]. The screening might not uncover that.
Mr. STUPAK [continuing]. Is your screening and even this guide here just for honest people? Keeping honest people honest?
Mr. ROUSH. I believe——
Mr. STUPAK. I mean, people who want to do us harm or terrorists, they don't care what—they aren't going to give you an honest answer. Right?
Mr. ROUSH. I think it is a valid question. What I would say is if you make the red flags in those processes robust enough, they start to triangulate in a way that unless somebody is extremely informed and diligent, they are going to become fearful as Mr. Fitton said, and back away from the transaction, or you will start to detect that in their behavior.
Mr. STUPAK. Well, you know, here GAO made up a fictitious company, it had fictitious reason for wanting these trigger spark gap, and its promise was not to export, and then your company sort of relied upon those statements or misstatements, but we didn't go any further to try to verify that. Right? Your company?
Mr. ROUSH. That is correct.
Mr. STUPAK. OK. Mr. Kutz, did Perkin Elmer conduct any verification on the representations you made? Do you know? Did you know if anyone tried to verify what you had said or put down? In your own—anything come back to you?
Mr. KUTZ. I don't know exactly what they did. I—there was no end-use certificate on that one as I understand, but we did meet with their folks, and they do have a compliance group, and so, again, there was no violation of the law, and their processes seemed to be consistent with some other companies we dealt with, the bigger companies.
Mr. STUPAK. OK. Mr. Roush, if I could go back to you there on this spark plug and—I am sorry. Spark—yes. You submitted with your testimony an article from the Boston Globe describing a real case which your company cooperated with law enforcement officials to thwart an illegal shipment of trigger spark gaps to Pakistan in 2003.
Mr. ROUSH. Correct.
Mr. STUPAK. According to this article it was—the size of the order was 200 spark gaps, which is enough to detonate three to ten nuclear bombs, that caused your company to alert law enforcement, and one of your spokesmen said, "It was such a huge quantity, a hospital buys one or two." Is that correct?
Mr. ROUSH. Those statements are correct, and I would say that particularly the geographic region of the world affects whether you

would view a quantity as valid or not for medical purposes, because in the United States the healthcare infrastructure is much larger. So it is normal that customers in the United States might order, you know, as many as a few hundred of these, particularly if they were a distributor serving multiple hospitals.

Mr. STUPAK. But you would know those customers, wouldn't you? Pretty much?

Mr. ROUSH. Typically that is correct. Yes.

Mr. STUPAK. So then Mr. Kutz, before you made your purchase from Mr. Roush's company, Perkin Elmer, you asked him for a quote on a larger order of trigger spark gaps. Right?

Mr. KUTZ. One hundred. Yes.

Mr. STUPAK. OK, and so you had a totally new customer then asking for 100, Mr. Roush, that you never dealt with before, and they were seeking 100 spark gaps, why didn't that alert you, or why didn't you have law enforcement check these guys out?

Mr. ROUSH. This is actually a completely normal practice for our new customers in all of our product lines, including trigger spark gaps, that normally a customer will buy one sample of something and test that under an R&D or development process. And if it does then meet their specifications, they are going to want to purchase production quantities of that, so we will typically provide the pricing for the sample and the pricing for the production quantity upfront. That is the normal, competitive practice, and it was followed in this case, and in fact, this, you know, fictitious company indicated they wanted one piece for development purposes, and if that worked in the application, then further quantities would be ordered at that time, and you know, there would be a separate transaction that would be screened in its own right at that time.

So this was a normal commercial practice.

Mr. STUPAK. Any comments?

Mr. KUTZ. That could very well be true. I mean, we didn't want to spend $70,000 instead of $700.

Mr. STUPAK. Right.

Mr. KUTZ. That was really the reason we did it that way.

Mr. STUPAK. OK. What would you use—what would a company buy 100—what would you use 100 for? I guess I am still trying to figure this one out.

Mr. ROUSH. Well, because this part is used in the lithotripter treatment devices in hospitals around the United States, there is an awful lot of hospitals—it is—there are spare parts demands as well as new system demands that we sell 2,000 of these devices in a year, in excess of 2,000, and 70 percent of those are for medical uses. So the quantity of, you know, one now and potentially 100 later is not at all unusual.

Mr. STUPAK. I see. So it wasn't the fact that 100, it was that they had wanted one for research and then might possibly want 100 more?

Mr. ROUSH. Correct, and so we provided standard quantity pricing for various quantities that would be ordered. That is the normal practice. Nobody will design your component into a system if they have no idea what they are going to be paying once they go into production, because they have to work towards, typically to-

wards some kind of cost for that system, and they want to know for planning purposes what your price would be.

Typically there is a volume discount——

Mr. STUPAK. Right.

Mr. ROUSH [continuing]. You know.

Mr. STUPAK. But wouldn't you then sort of ask like, OK, I got my one for research and—or for testing purposes but then when I asked for 100, wouldn't you usually ask what the product is? In this case you never even asked what they were going to use the 100 for, did you?

Mr. ROUSH. Well, in this case we did not, but I will tell you that, you know, triggered spark gaps are not one thing. It is a product group. OK. We offer a lot of different models. Most of them are specifically designed for a range of performance of a medical device. So some of them operate at 20 kilobolts, some at 10 kilobolts, 12. The military versions we sell typically operate at 2 kilobolts. There is no overlap in the operating range, so there was nothing about this that would have indicated that it was for use in some sort of, you know, munitions application. It was entirely consistent with our medical versions.

Mr. STUPAK. Sure, and there is no requirement under law since it was domestic to make sure they were licensed, and there is no requirement to follow up to end user or anything like that. Right?

Mr. ROUSH. Correct.

Mr. STUPAK. Mr. Gingrey, questions?

Mr. GINGREY. Mr. Chairman, thank you.

Let me go to Mr. Borman. Mr. Borman, some items can be exported to some countries without a license but require a license if going to certain other countries. Some items can be exported to some countries as long as they are intended for commercial purposes but not for military purposes. Some items can't be exported to some countries for any reason.

I think you are getting my drift here. With all of the variables and exceptions, is it not—and I think it is but I want your answer, is it not confusing for government agencies and businesses involved in export and export controls to make sure everyone is doing the right thing? Do you know?

Mr. BORMAN. Well, that is a very good question, sir, and it is a complex system, and I think it has evolved that way because of what I mentioned earlier. Last year, for example, there were $1.3 trillion worth of exports from the United States. Probably the vast majority of those are subject to our regulations but have gradated requirements, depending on what the item is and where and who it is going to.

And so off the top of my head certainly the system could be made simpler but to make it simpler I think it has to go one of two ways. Either you drastically reduce requirements for items and places or you drastically increase the level of control. And when you are talking about a, you know, $1.3 trillion worth of exports, that would have a significant impact.

And so that is why the system has evolved to try to give exporters more and more information about the types of transactions and the technologies that they need to be most concerned about.

Mr. GINGREY. Well, you earlier before we went to vote, there was, I think Mr. Burgess from Texas was questioning why the dual system or responsibility when you, of course, have the Department of State and Department of Commerce, the Department of Commerce controlling these products that are dual use, and Department of State controlling those that are just for military purposes and military sales, and you got into some discussion, actually, any one of the three of you, Mr. Kutz, Ms. Lasowski, Mr. Borman, let us elaborate that a little bit more, if you will. Because I think what Burgess was getting at was to simply, to make it so that the right hand will know what the left hand is doing, the left hand will know what the right hand is doing, it would be a more efficient way and less chances for sales that would be inappropriate.

Let us talk about that a little bit in my remaining time and throw it open to the GAO.

Ms. LASOWSKI. I think you have raised some excellent questions because the system that was created decades ago was——

Mr. GINGREY. How long ago would you say the system was created?

Ms. LASOWSKI. Well, the current laws were established in their most recent form in the 1970s, but they do date back earlier in different forms.

Mr. GINGREY. I think you said back into the 1940s earlier, didn't you?

Ms. LASOWSKI. There—that is where there was an origination, yes, but the current laws that are in existence really were in the 1970s, and there hasn't been a major overhaul of these particular laws, and has previously mentioned, the Export Administration Act is currently lapsed.

So it is fair that in terms of a reexamination, which is what we have been calling for, that it would be appropriate to take a look at the current challenges that have been evolving for the 21st century and reexamine the system to look at the very basic questions; what is it that needs to be controlled and how do we want to control it. And then establish clear lines of responsibility and accountability for how best to do that.

And so those would be I think the fundamental aspects of such a reexamination.

Mr. GINGREY. Mr. Kutz, any comment? Mr. Borman?

Mr. BORMAN. I think that—I generally agree with that. To add a little bit of, I guess, fuel to the fire to your concern about the complexity, we are talking about dual use in munitions items, but there are actually several other agencies that have direct authority to regulate the control of other exports. For example, the Nuclear Regulatory Commission on their Atomic Energy Act controls the export of nuclear materials and equipment. Department of Energy has specific authority.

So it seems more complicated, although these are the two main systems. But clearly the current threat challenges, technologies and markets, are really challenging the system as it currently exists.

Mr. GINGREY. Yes, you know, and just continue along that same line and all these variables and exceptions, is it not confusing for government agencies and businesses involved in exports and export

controls to make sure everyone is doing the right thing? I mean, that is my main point.

Mr. BORMAN. It is certainly a challenge. That is why we do so much on outreach, for example. We do 30, 40, 50 outreach events every year throughout the country just BIS, and there is a whole cottage industry of private entities that do export control compliance seminars, I think in part as a reaction, a market reaction to that.

Mr. GINGREY. Are some dual-use items more sensitive than others?

Mr. BORMAN. Oh, certainly. Certainly. I mean, there is a whole strata of—most of what we control on our controllers are based on multi-lateral agreements by most of the supplier countries. There is one specific, the Nuclear Missile Technology Cambio and sort of conventional arms, and then there is another strata that are controlled really just to the terrorist countries or to specific bad end users in different countries.

So there is certainly a large gradation.

Mr. GINGREY. You touched on the fact that a number of different laws and regulations, agencies, multi-lateral agreements play a role in how we control our exports. Can you describe some of the challenges that this presents?

Mr. BORMAN. Well, absolutely. I mean, on the multi-lateral side there is agreement, again, among most but not all suppliers as to items to be listed but then certainly each country has individual discretion as to how they actually implement those controls. And what we hear a lot from U.S. industry is that our system is much more rigorous than other countries, and therefore, they are at a competitive disadvantage when they are selling into markets like China and India, for example.

So that is a real challenge. Another real challenge, of course, is what we call foreign availability. It was alluded to earlier. There are—many of the things we control are available from many countries including the countries that are the target of those controls. So——

Mr. GINGREY. Mr. Borman, thank you, and Mr. Chairman, I yield back to you at this point.

Mr. STUPAK. Thanks. Just a couple of questions if I may.

Mr. Kutz, if I could ask you, have you got the book there, the document binder there? I want to look at tab number three, because one of the things that caught my attention, you mentioned in your testimony that one seller actually signed up your fake company as a reseller or dealer. That was on the night vision. Is that right?

Mr. KUTZ. It was a distributor. It wasn't the manufacturer.

Mr. STUPAK. OK. No, no. It was the distributor. Right. Not the manufacturer. So if you look at tab three, which is the reseller dealer agreement between GAO's fictitious company and a company called KERIF Night Vision.

Mr. KUTZ. Correct.

Mr. STUPAK. Whose idea was it to make your company, your false company a dealer of night-vision equipment?

Mr. KUTZ. It was the only way we could get the item. They wouldn't sell it to us otherwise, so we agreed to fill out this agreement, and that was the way we got the items.

Mr. STUPAK. OK. So in order to obtain the item you had to fill out this dealer, reseller, dealer——

Mr. KUTZ. Reseller, dealer agreement was necessary to get our target item. Yes.

Mr. STUPAK. What information were you required to provide to become a dealer?

Mr. KUTZ. Well, it was interesting. We didn't have to provide a Social Security number or an EIN, and that would be something, you know, employer identification number. It was other information, you know, name, address, and I believe other information, but it wasn't any personably identifiable information.

Mr. STUPAK. Well, did you have a face-to-face meeting with this company?

Mr. KUTZ. Yes, we did. No, we did not. Not until afterwards. No.

Mr. STUPAK. OK.

Mr. KUTZ. Afterwards. We actually met with this individual afterwards.

Mr. STUPAK. After. So before you became a dealer you never even had a face-to-face meeting with this company that was going to make you a dealer of their night vision?

Mr. KUTZ. That is correct.

Mr. STUPAK. OK. What is your understanding of what access to night-vision equipment would you have as a dealer?

Mr. KUTZ. Well, I guess ITT could probably better answer that because it was ultimately their product, but we were at several levels below the distributor level so——

Mr. STUPAK. OK.

Mr. KUTZ [continuing]. Our understanding was we could have actually purchased more of these from this individual. That was one of the discussions, I believe, we had. We don't know how many or under what circumstances.

Mr. STUPAK. OK, and Mr. Alvis, I realize that your company, you are the manufacturer and there is probably multiple layers between you and this KERIF Night Vision. Do you know how many layers that would be between you and probably KERIF? Two or three?

Mr. ALVIS. My guess is the company that sold to them——

Mr. STUPAK. Right.

Mr. ALVIS [continuing]. Is probably one of our three dealers because——

Mr. STUPAK. OK.

Mr. ALVIS [continuing]. They do have 25 distributors, now 26.

Mr. STUPAK. But before you ever would deal with them, would there be a couple layers?

Mr. ALVIS. We wouldn't deal with——

Mr. STUPAK. KERIF?

Mr. ALVIS [continuing]. Anybody. We deal with three companies——

Mr. STUPAK. And then they——

Mr. ALVIS [continuing]. That we are allowed to audit.

Mr. STUPAK. OK.

Mr. ALVIS. As I mentioned earlier, we haven't audited them, however, we do cooperate with law enforcement, FBI whenever—obviously as the biggest manufacturer whenever there is an investigation, we cooperated with GAO on this end.

We are a resource, and every time we have gone to one of our dealers, all their paperwork has been right on the money. So the end-use statements that we put out there, whenever we have had to follow up, they have always had all the paperwork and all the documentation.

Mr. STUPAK. Well, I take it from your answer then KERIF had no requirement of contacting you and saying, hey, I signed up a new company to sell night vision.

Mr. ALVIS. No.

Mr. STUPAK. OK.

Mr. KUTZ. Mr. Chairman, I would just say, too, ITT was able to trace this item down within a couple of hours, very quickly.

Mr. STUPAK. By going through——

Mr. ALVIS. We make 175,000 night-vision tubes a year. Every tube we make is serial numbered whether it is going to the U.S. military. Everything we do is ITAR, so we don't have the dual-use distinction. Everything is ITAR. The downgraded tubes or the non-military spec tubes that we sell into the commercial market are also serial numbered. So whenever GAO—and that is a very—that—there is 2 generations behind that goggle up there on the front is 2 generations behind what the U.S. Army currently has. We could still take that serial number. We can also autopsy any tubes and see what has been done to it.

Mr. STUPAK. Sure. Let me ask you this in tab three, and you may want to pass that down to him, in there it says, "KERIF shall exercise no control over the activities and operations of reseller, dealer." In other words, Mr. Kutz's company there with the GAO.

Have you ever seen these agreements like that? Is that something your distributors do, where they shall exercise no control over the activities and operations of a reseller, dealer?

Mr. ALVIS. I have actually never looked at a dealer agreement that came from one of our distributors to a lower-level distributor.

Mr. STUPAK. OK.

Mr. ALVIS. However, I will see if our team—Greg, have you ever looked at——

Mr. STUPAK. He can't answer. He would have to answer through you, sir. He can advise you but he can't——

Mr. ALVIS. Oh. OK. Fine.

Mr. STUPAK. It is also on the board up there, too.

Mr. ALVIS. KERIF, even though they are the distributor——

Mr. STUPAK. KERIF. OK.

Mr. ALVIS. Yes. KERIF. They gave the agreement to the fictitious company.

Mr. STUPAK. Right.

Mr. ALVIS. They are not the one—they are not our dealer. So there is——

Mr. STUPAK. Right.

Mr. ALVIS [continuing]. A layer in there.

Mr. STUPAK. There is a layer in there.

Mr. ALVIS. And that layer in there is required to have the end-use statements and all the documentation that we are likely to audit and occasionally call on them to give back to us in cooperation with law enforcement.

Mr. STUPAK. OK. I guess the part that gets me a little bit is the law prohibits exports of your product outside the United States, but when it is—but when you hire a distributor, you don't control who that distributor signs up as dealers of your product. So the distributor signs up a dealer and doesn't control the activities of the dealer. So it sounds like we got a crazy system here. You can't export, you hire a distributor, he hires dealers, and everyone says we exercise no control over the activities of the next person.

Go ahead.

Mr. ALVIS. This distributor, this real-world distributor, not the fictitious company——

Mr. STUPAK. Right.

Mr. ALVIS [continuing]. Would be the distributor that hired him, would be in violation of our agreement.

Mr. STUPAK. Of your agreement?

Mr. ALVIS. Of our agreement.

Mr. STUPAK. OK.

Mr. FITTON. Mr. Chairman.

Mr. STUPAK. Sure.

Mr. FITTON. As a dealer myself in night-vision goggles and equipment, the certificates that I signed as a dealer setting up myself as a distributor or dealer for the company I have to agree not to export the items through any distributor I purchase it through. So even down to my level giving it to the end user I have to abide by these same laws and regulations.

Mr. STUPAK. Sure, because you are in the United States, but then after you sell it to someone, they can do anything they want with it in a way.

Mr. FITTON. Correct. Once it falls into civilian hands, then it is out of our control.

Mr. STUPAK. OK. Thanks.

Mr. Gingrey, anymore questions? Wrap it up here.

Mr. GINGREY. Mr. Chairman, thank you. I did have a couple more that I wanted to address to the GAO, Mr. Kutz or Ms. Lasowski, excuse me.

In my State of Georgia we—in fact, in my Congressional district even we have a large number of defense contractors and businesses, both large and small, who work every day in good faith towards the defense of our Nation as well as the defense of our international allies, which is also in our own national defense.

While there are clearly areas upon which we need additional oversight, it also seems that many of these small businesses that I represent, who play by the rules, experience sometimes massive delays when trying to secure the necessary licensing through the State Department and its Directorate of Defense Trade Controls.

So my first question is this. As a result of your investigation do you have any insight with respect to the existing process at the Directorate and its efficiency in approving clearly, clearly aboveboard export activities, how timely do you believe the Directorate is in the approval process? How long should American businesses be ex-

pected to wait in this process, because time is money obviously. They lose these opportunities if it drags on too long, and I have had one of these companies come to me with this concern.

Mr. KUTZ. Yes. Nothing we did in the investigation was aboveboard, so I will pass.

Ms. LASOWSKI. Over the years we have looked at the State Department——

Mr. GINGREY. Is your mike on, Ms. Lasowski?

Ms. LASOWSKI. Over the years——

Mr. GINGREY. You got a sweet, low voice.

Ms. LASOWSKI. Oh, thank you. Let me see if I can speak up a little bit here.

Mr. GINGREY. That is fine.

Ms. LASOWSKI. Over the years we have looked at the State Department's licensing process, and we have noted a number of inefficiencies associated with the process. We have recognized that it is important for the process to take the time necessary to deliberate and to do various verifications and come up with the appropriate restrictions that will be placed on the licensed conditions for the exports.

However, we have noted that a number of inefficiencies have delayed the process, and a couple of years ago when we looked at the process, we noted that there were not particular standard operating procedures, there was not a lot of attention in terms of the—taking a triage approach in terms of referring the licenses to the appropriate parties.

So when we completed our review, we made a number of recommendations to improve the efficiency of the licensing process. We have not been back into examine the current state of play, however, we have been briefed by State Department officials that they have taken a number of steps to restructure their workforce and to establish procedures and training in an attempt to reduce the number of licenses that are in the pipeline and also to ensure that they are consistent in terms of their processing with license applications.

Mr. GINGREY. Well, I appreciate that answer. I would suggest to you that the problem is still there, and my information is very, very recent, and I sincerely do believe the problem is still there.

Is this applicable as well to the Department of Commerce? You mentioned the Department of State but——

Ms. LASOWSKI. In terms of the Department of Commerce, most of the exports can occur without an actual license application. So very few in terms of what is ultimately under the control is licensed and compared to a much larger volume of licensed applications that occur at the State Department.

Mr. GINGREY. I see. Sure. Of course. That makes sense. Well, thank you all very much. I appreciate the opportunity to hear from you and ask you some questions.

And I thank you, Mr. Chairman. I yield back to you.

Mr. STUPAK. Thank you, Mr. Gingrey.

As I said, we started this investigation in 2008. We are going to continue our investigation. I want to emphasize again that the witnesses that have appeared here today, they have created no violation of law. ITT, Perkin Elmer, and Mr. Fitton, you guys followed

the law, you did not violate the law, and you probably followed the absence of law as I think Mr. Walden said earlier.

So that is work for this committee to do some more work, and I want to thank you for your cooperation in providing the requested documents as well as the other companies that were part of this sting operation that did provide documents to us.

And I just—I have to for the record note there is one exception. Systron Donner of Walnut Creek, California, a company which sold the GyroChips to the GAO undercover company, that company, Systron Donner, stands out for defiant failure to comply with the document request from our committee. While everybody else complied with it, they refused to—and we are going to continue to press to receive the information from this company.

So I want to thank you for your being here, thank you for your cooperation, thank you for your testimony, and thank all of our witnesses. And that concludes our testimony for today.

The rules provide that members have 10 days to submit additional questions for the record. I ask unanimous consent that the content of our document binder be entered into the record, provided that the committee staff may redact any information that is of business proprietary nature or relates to privacy concerns or is a law enforcement sensitive in nature.

Without objection, the documents will be entered in the record.

That concludes our hearing. The meeting of the subcommittee is adjourned.

[Whereupon, at 1:15 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

ITT Response to Cong. Bruce Braley's Inquiry in Oversight Hearing of 6/4/09

Administrative Export Enforcement Matter Involving Engineered Valves Group of ITT Corporation

Q: "This isn't the only time your company has engaged in illegal export activities. The Committee requested from the Department of Commerce copies of documents related to other ITT export violations. One document shows that in 2007, one of your subsidiaries , Engineered Values Group, was fined for illegally shipping valves used in chemical and biological weapons to China, Israel, Saudi Arabia and Taiwan. Isn't that right?"

This is submitted in response to a question posed by Congressman Braley to a representative of ITT-Night Vision at the June 4, 2009, House Energy and Commerce Subcommittee hearing on Commercial sales of Military Technologies. Specifically, Congressman Braley asked Mike Alvis, Vice President of Business Development for ITT-Night Vision whether he was aware that another subsidiary of ITT, Engineered Valves, had been fined in 2007 for illegally shipping valves used in chemical and biological weapons to China, Israel, Saudi Arabia and Taiwan. Mr. Alvis responded that he was unaware of both the incident and the particular entity involved and that ITT would respond for the record after examining the details.

ITT is an international company that consists of in excess of six hundred business entities. These business entities are divided among our ITT-Defense Systems (Defense) and ITT-Fluids and Motion and Flow (Commercial) Groups. Engineered Valves (EV) is a business unit within the Industrial Process Division of ITT - Fluids and Motion and Flow. Night Vision, on the other hand, is part of ITT - Defense Systems, which explains why Mr. Alvis was unaware of this particular matter.

In 2007, ITT entered into an administrative settlement with the Commerce Department's Bureau of Industry and Security (BIS) relating to the unlicensed export by EV of six (6) shipments of valves and valve bodies to China, Israel, Taiwan and Saudi Arabia between February, 2001 and August, 2005. The violations were discovered during an internal investigation by Engineered Valves of some 3,200 export transactions involving controlled products which occurred during this five year period. The shipments were voluntarily self-reported by ITT to BIS in disclosures dated June 27, 2005 and January 31, 2006. All of the violations were inadvertent and involved valves that either had been previously or would have been approved by BIS for export to the customers in these four countries. The total value of the shipments was less than $16,000, as compared to approximately $40 million in export sales by Engineered Valves during this time frame. Under the terms of the settlement agreement, Engineered Valves was assessed and paid a civil penalty in the amount of $26,400. Independently, it established and implemented extensive corrective actions to ensure that similar mistakes would not occur in the future.

Of the six unlicensed shipments self-reported to BIS by EV, three occurred in 2001 and involved the failure to obtain licenses for products that Engineered Valves had previously sought and obtained approval from BIS to export to the ultimate end-users in Taiwan and Saudi Arabia. Two of the remaining shipments involved products that Engineered Valves

had mistakenly classified as not requiring an export license. ITT believes that as properly classified, these products would have been approved for export to the countries of ultimate destination, Israel and China, as licenses for similar products to these destinations had been approved by BIS in the past. The final unlicensed shipment self reported by EV involved a valve body product which was sent to a vendor in China in 2004 as a sample for the purpose of qualify and obtaining a quote from the vendor to manufacture the product. The product was returned to the United States in 2005 when the error was detected. It is ITT's belief that BIS would have approved the export of this shipment to the Chinese vendor had EV applied for a license. ITT was unaware of valves being used for any prohibited end use.

ITT is firmly committed to compliance with the export controls laws and regulations of the United States. That commitment is reflected in the actions taken by EV to detect, report and correct its export transgressions and in the extensive compliance program that ITT has put in place company-wide to ensure that its business transactions comport in every way with the requirements of the law. All of our Value Centers have export compliance groups which handle and monitor export activities on a daily basis under the guidance of a centralized office staffed by subject matter professionals. These individuals have been fully empowered by the company's senior leadership, which for the last three years has made compliance the number one priority of the company.

○